



EDS-MD Wired IoT Gateway for Medical Devices Command Reference

◆EDS-MD 4

◆EDS-MD 8

◆EDS-MD 16

Intellectual Property

© 2023 Lantronix, Inc. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix, EDS-MD, ConsoleFlow, and TruPort are registered trademarks of Lantronix, Inc. in the United States and other countries. DeviceInstaller and Com Port Redirector are trademarks of Lantronix, Inc.

Patented: patents.lantronix.com; additional patents pending

Windows is a registered trademark of Microsoft Corporation. All other trademarks and trade names are the property of their respective holders.

Contacts

Lantronix, Inc.

48 Discovery, Suite 250

Irvine, CA 92618, USAToll Free:800-526-8766

Phone: 949-453-3990 Fax: 949-453-3995

Technical Support

Online: www.lantronix.com/technical-support

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about-us/contact.

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

The EDS-MD wired IoT device gateway is not a medical device as such term is defined in the U.S. Food, Drug and Cosmetic Act, as amended, and is not subject to regulation by the U.S. Food and Drug Administration (FDA).

Revision History

Date	Revision	Comments	
September 2011	Α	Initial Document. Created for the 7.2.0.0 release.	
April 2015	В	Updated to firmware release 7.2.0.3.	

Date (continued)	Revision	Comments
May 2019	С	Updated to firmware release 8.1.0.3 which includes the addition of the following:
		Gateway port forwarding, static routes and DHCP serverSupport for NTP in clock
		 Support for Action settings Ethernet ports work separately
		Support for MACH10 client
September 2019	D	Updated to firmware release 8.1.0.4.
March 2023	Е	Updated to firmware 8.3.0.0R4 which includes the following changes and additions. Renamed Mach10 to ConsoleFlow Added TLS1,2 support
		Updated to firmware 8.4.0.0R4 which includes the following changes and additions.
		◆ Added SNMP◆ Added Modbus

Table of Contents

Intellectual Property	·
Contacts	2
Disclaimer	
List of Figures	
List of Tables	
1: About This Guide	7
Chapter Summaries	7
Conventions	
Additional Documentation	
2: Overview	g
XML Architecture and Device Control	(
Command Line Interface	
3: Command Line Interface	10
Configuration Using Telnet	10
Configuration Using Serial Lines	
Boot to CLI and Device Recovery	11
Navigating the CLI Hierarchy	11
Using Keyboard Shortcuts and CLI	12
Understanding the CLI Level Hierarchy	12
4: Configuration Using XML	15
XML Configuration Record Document Type Definition	15
Quick Tour of XML Syntax	16
Declaration	16
Element Start and End Tags	16
Element Attributes	16
	17
Importing and Exporting an XML Configuration File	
Best Practices	19
Importing	19
Exporting	
XML Configuration Groups	
XML Status Record Groups and Items	36
5: Commands and Levels	46

List of Figures

Figure 3-2 CLI Level Hierarchy	13
Figure 3-3 Login Level Commands	13
Figure 3-4 Enable Level Commands	14
Figure 4-1 DTD for XCRs	15
Figure 4-2 XML Example	16
Figure 4-3 XML Example	17
Figure 4-4 XML Example of Multiple Named Values	17
Figure 4-5 XML Example of Multiple Items	18
Figure 4-6 XML Example with Multiple Groups	18

List of Tables

Table 3-1 Keyboard Shortcuts	·	12
Table 4-7 XCR Groups		21
Table 4-8 XSR Group and Items		36

1: About This Guide

This guide describes how to configure the Lantronix® EDS-MD® wired IoT device gateway using the Command Line Interface (CLI) and/or Extensible Markup Language (XML). CLI provides an interactive mode for accessing the device configuration and management interface. It is most suited for system and network administrators comfortable with using similar interfaces on Enterprise IT and Networking products. It is also helpful as a quick tool for access via the product's serial ports or console/management ports.

XML provides an extensible mode for software developers interfacing with the device and system integrators performing batch provisioning/updates.

Note: EDS-MD wired IoT device gateways (which include models EDS-MD 4, EDS-MD 8 and EDS-MD 16) are commonly referred to as either EDS-MD 4/8/16 or as EDS-MD when mentioned within a description equally applicable to any of the three models.

Chapter Summaries

This table lists and summarizes content of each chapter.

Chapter	Summary		
Chapter 2: Overview	Gives an overview of CLI and XML.		
Chapter 3: Command Line Interface	Lists commands and describes how to use CLI to configure the EDS-MD 4/8/16 wired IoT device gateways.		
Chapter 4: Configuration Using XML	Lists XCR groups and items and describes how to use XCRs to configure the EDS-MD 4/8/16 wired IoT device gateways.		
Chapter 5: Commands and Levels	Provides an index of the CLI Command Hierarchy with hyperlinks to the corresponding command details.		

Conventions

The table below lists and describes the conventions used in this book.

Convention	Description		
Bold text	Default parameters.		
Italic text	Required values for parameters		
Brackets []	Optional parameters.		
Angle Brackets < >	Possible values for parameters.		
Pipe	Choice of parameters.		
Warning	Warning: Means that you are in a situation that could cause equipment damage or bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.		
Note	Note: Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.		

Convention (continued)	Description		
Caution	Caution: Means you might do something that could result in faulty equipment operation, or loss of data.		
Screen Font (Courier New)	CLI terminal sessions and examples of CLI input.		

Additional Documentation

Visit the Lantronix website at www.lantronix.com/resources/product-index/ for the latest documentation and the following additional documentation.

Document	Description	
EDS-MD Wired IoT Device Gateway User Guide	Describes how to configure and use an EDS-MD 4/8/16 wired IoT device gateway.	
Com Port Redirector Quick Start and Online Help	Instructions for using the Lantronix Windows based utility to create virtual com ports.	
Lantronix Provisioning Manager User Guide	Instructions for using Lantronix Provisioning Manager to discover, configure, upgrade, and manage an EDS-MD 4/8/16 wired IoT device gateway.	

2: Overview

The EDS-MD 4, EDS-MD 8 and EDS-MD 16 wired IoT device gateways support three convenient configuration methods: Web Manager, Command Line Interface (CLI) and Extensible Markup Language (XML). For more information about the Web Manager, see the *EDS-MD Wired IoT Device Gateway User Guide* on the Lantronix website.

XML Architecture and Device Control

XML is a fundamental building block for Machine-to-Machine (M2M) and Internet of Things (IoT) networks. The EDS-MD 4/8/16 wired IoT device gateway supports XML configuration records that make configuring the wired IoT device gateway easy for users and administrators. XML configuration records are easy to edit with a standard text editor or an XML editor.

For a brief overview of XML, see *Chapter 4: Configuration Using XML*. It provides rules on basic XML syntax, a guide to the specific XML tags used, and a guide to using XML configuration records.

Command Line Interface

The EDS-MD 4/8/16 wired IoT device gateway uses industry-standard tools for configuration, communication, and control. For example, the EDS-MD 4/8/16 wired IoT device gateway uses a command line interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

For details of the CLI, see *Chapter 5: Commands and Levels*. It provides an index of the CLI Command Hierarchy with links to the corresponding command details. The CLI provides commands for configuring, monitoring, and controlling the wired IoT device gateway.

3: Command Line Interface

This chapter describes accessing the EDS-MD 4, EDS-MD 8 or EDS-MD 16 wired IoT device gateway by using Telnet or serial ports to configure the device, navigating the Command Line Interface (CLI), typing keyboard shortcuts, and moving between the levels.

It contains the following sections:

- Configuration Using Telnet
- Configuration Using Serial Lines
- Navigating the CLI Hierarchy
- Using Keyboard Shortcuts and CLI
- Understanding the CLI Level Hierarchy

Refer to *Chapter 5: Commands and Levels* for a complete list of levels, commands, and descriptions.

Configuration Using Telnet

To access and configure the wired IoT device gateway by using a Telnet session over the network, you must first establish a Telnet connection. You can also establish a Telnet connection by clicking the Telnet Configuration tab in the Lantronix® DeviceInstaller™ utility. See the DeviceInstaller Online Help for more information, available on our website www.lantronix.com/support/downloads.

To access the EDS-MD 4/8/16 wired IoT device gateway by using Telnet, perform the following steps.

- 1. Click Start > Run. The Run dialog box displays.
- 2. Type cmd in the dialog box and press **OK**.
- 3. Type telnet x.x.x.x (x.x.x.x is the IP address) in a Windows/Linux command prompt.
- 4. The EDS-MD 4/8/16 wired IoT device gateway is online when the command prompt (>) displays. You are at the root level of the CLI.

Note: Depending on the level of security, a password may be required.

Configuration Using Serial Lines

Serial Port Command Line Mode

The serial port can be configured to operate in command mode permanently or to be triggered under specified conditions. See the line line> Level command description for more information.

In order to configure and manage the device, connect the computer via a Serial (RS232) cable to the EDS-MD unit and run a terminal emulation program (e.g., Tera Term). Reference the EDS-MD Wired IoT Device Gateway User Guide for additional information on connecting the serial port prior to configuration.

Boot to CLI and Device Recovery

Serial Recovery mode will temporarily override the line and tunnel settings for the serial line to allow configuration changes to be made. The line and tunnel settings will be restored once the user exits the Serial Recovery mode CLI.

To configure the EDS-MD wired IoT device gateway locally using a serial port:

- 1. Connect a terminal or a PC running a terminal emulation program to one of the wired IoT device gateway's serial ports.
- 2. Configure the terminal to the following settings:
 - 9600 baud
 - 8-bit
 - No parity
 - 1 stop bit
 - No flow control.
- 3. Power off the device.
- 4. Press and hold down the exclamation point (!) key.
- 5. Power on the device. After about 5 seconds, the exclamation point will display on the terminal or PC screen.
- 6. Type xyz within 5 seconds to display the CLI prompt.

Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of levels. Each level has a group of commands for a specific purpose. For example, to configure a setting for the FTP server, one would navigate to the FTP level, which is under the configuration level.

- ◆ To move to a different level—Enter the name of the level from within its parent level. For example, to enter the tunnel level, type tunnel <number> at the enable prompt. This displays: <enable> tunnel <number>#.
- To exit and return to one level higher—Type exit and press the Enter key. Typing exit at the login level or the enable level will close the CLI session. If Line - Command Mode is specified as Always, a new session starts immediately.
- To view the current configuration at any level—Type show.
- ◆ To view the list of commands available at the current level—Type the question mark "?". Items within < > (e.g. <string>) are required parameters.
- ◆ To view the available commands and explanations—Type the asterisk (*).
- To view the list of commands available for a partial command—Type the partial command followed by the question mark "?". For example: <tunnel-1>#show? displays a list of all show commands at the tunnel level.
- ◆ To view available commands and their explanations for a partial command—Type the partial command followed by the asterisk (*). For example: <tunnel-1>#show* displays a list of all show commands and descriptions at the tunnel level.
- To view the last 20 commands entered at the CLI—Type show history.

Using Keyboard Shortcuts and CLI

One useful shortcut built into the EDS-MD 4/8/16 wired IoT device gateway is that the complete text of a command does not have to be entered to issue a command. Typing just enough characters to uniquely identify a command, then hitting enter, can be used as a short cut for a command. For example, at the enable level, "sh" can be used for the "show" command.

Tab Completion is also available using the **Tab** and **Enter** keys on the keyboard. Typing the first few characters of a command, then hitting the **Tab** key displays the first command that begins with those characters. Hitting the **Tab** key again displays the next command that begins with the original characters typed. You can press **Enter** to execute the command or you can backspace to edit any parameters.

The following key combinations are allowed when configuring the wired IoT device gateway using the CLI:

Key Combination	Description	
Ctrl + a	Places cursor at the beginning of a line	
Ctrl + b	Backspaces one character	
Ctrl + d	Deletes one character	
Ctrl + e	Places cursor at the end of the line	
Ctrl + f	Moves cursor forward one character	
Ctrl + k	Deletes from the current position to the end of the line	
Ctrl + I	Redraws the command line	
Ctrl + n Displays the next line in the history		
Ctrl + p	Displays the previous line in the history	
Ctrl + u	Deletes entire line and places cursor at start of prompt	
Ctrl + w	Deletes one word back	
Ctrl + z	Exits the current CLI level	
Esc + b	Moves cursor back one word	
Esc + f	Moves cursor forward one word	

Table 3-1 Keyboard Shortcuts

Understanding the CLI Level Hierarchy

The CLI hierarchy is a series of levels. Arranging commands in a hierarchy of levels provides a way to organize and group similar commands, provide different levels of security, and reduce the complexity and number commands and options presented to a user at one time.

When you start a command line session, you begin at the login level. This level can be password protected and provides access to high level status, a few diagnostic commands, and the enable level. Further device information and configuration are accessed via the enable level.

The enable level can also be password protected and is the gateway to full configuration and management of the wired IoT device gateway. There are commands for gathering and effecting all elements of device status and configuration, as well as commands that take you to additional levels. For instance, tunnel specific status and configuration is found under the "tunnel" level, and network specific status and configuration commands are found under the "configuration" level.

Figure 3-2 CLI Level Hierarchy enable configure (login) action arp device cli dns telnet clock email <number> consoleflow filesystem log diagnostics line <line> discovery ftp server gateway ssl credentials host trusted <number> authorities http tunnel accept icmp connect eth0 link <instance> disconnect eth1 link modem eth2 link packing ip serial modbus xml rss smtp snmp syslog line> terminal

An overview of the levels in the EDS-MD 4/8/16 wired IoT device gateway is presented in *Figure 3-2 CLI Level Hierarchy* below.

Commands at the login level (see *Figure 3-3 Login Level Commands* below) do not affect current configuration settings and are not displayed initially. If you type ?, you will see the login subcommands. These commands provide diagnostic and status information only.

Figure 3-3 Login Level Commands

Note: To configure the EDS-MD 4/8/16 wired IoT device gateway, you must be in the enable level and any of its sub-levels. Figure 3-4 below shows the enable level commands.

Figure 3-4 Enable Level Commands

```
>enable
(enable)#?
auto show interfaces
                                                             auto show processes
clrscrn
                                                             configure
connect
                                                             connect line <line>
device
                                                             disable
dns
                                                             email <number>
exit
                                                             filesystem
iperf <params>
                                                             kill ssh <session>
kill telnet <session>
                                                            line <line>
                                                           ping <host> <count>
ping <host>
ping <host> <count> <timeout>
                                                          reload
reload factory defaults
                                                            show
show history
                                                            show interfaces
                                                             show lines
show ip sockets
show processes
                                                             show sessions
ssh
                                                             ssh <optClientUsername> <host>
ssh <optClientUsername> <host> <port>
tcpdump <parameters>
                                                             telnet <host>
telnet <host> <port>
                                                             trace route <host>
trace route <host>                                                                                                                                                                                                                                                                                                                                                  
                                                            tunnel <line>
write
                                                             xml
(enable)#
```

See the *Chapter 5: Commands and Levels* at the end of this document for a complete list of levels, commands, and descriptions.

4: Configuration Using XML

The EDS-MD wired IoT device gateway provides an Extensible Markup Language (XML) interface that you can use to configure wired IoT device gateways. Every configuration setting that can be issued from the Web Manager and CLI can be specified using XML.

The wired IoT device gateway can import and export configuration settings as an XML document known as an XML Configuration Record (XCR). An XCR can be imported or exported via the CLI, a Web browser, FTP, or the wired IoT device gateway file system. An XCR can contain many configuration settings or just a few. For example, it might change all of the configurable parameters for a wired IoT device gateway, or it may only change the baud rate for a single serial line. Using XCRs is a straightforward and flexible way to manage the configuration of multiple wired IoT device gateways.

XML Configuration Record Document Type Definition

An XML document type definition (DTD) is a description of the structure and content of an XML document. It verifies that a document is valid. XCRs are exported using the DTD as shown in *Figure 4-1 DTD for XCRs*.

Figure 4-1 DTD for XCRs

```
<!DOCTYPE configrecord [
<!ELEMENT configrecord (configgroup+)>
<!ELEMENT configgroup (configitem+,configgroup*)>
<!ELEMENT configitem (value+)>
<!ELEMENT value (#PCDATA)>
<!ATTLIST configrecord version CDATA #IMPLIED>
<!ATTLIST configgroup name CDATA #IMPLIED>
<!ATTLIST configgroup instance CDATA #IMPLIED>
<!ATTLIST configitem name CDATA #IMPLIED>
<!ATTLIST value name CDATA #IMPLIED>
<!ATTLIST value name CDATA #IMPLIED>
```

The EDS-MD 4/8/16 wired IoT device gateway DTD rules state the following:

- The XML document element is a <configrecord> element. This is the root element.
- A <configrecord> must have one or more <configgroup> elements and can have a version attribute.
- A <configgroup> must have one or more <configitem> elements and can have name and instance attributes.
- A <configitem> element must have one or more <value> elements and can have a name attribute.
- A <value> element can have only data and can have a name attribute.
- The name attribute identifies a group, item, or value. It is always a quoted string.
- The instance attribute identifies the specific option, like the serial port number. The "instance" attribute is always a quoted string.

Note:

- The name for each <configgroup> (specified with the name attribute) is the group name listed in the Web Manager XCR groups or with the "xcr list" CLI command. See the EDS-MD Wired IoT Device Gateway User Guide for more information about the XCR groups.
- An empty or missing <value> element in each present <configgroup> clears the setting to its default.

Quick Tour of XML Syntax

Declaration

The first line, <?xml version="1.0" standalone="yes"?>, is called the XML declaration. It is required and indicates the XML version in use (normally version 1.0). The remainder of the file consists of nested XML elements, some of which have attributes and content.

Element Start and End Tags

An element typically consists of two tags: start tag and an end tag that surrounds text and other elements (element content). The start tag consists of a name surrounded by angle brackets, for example <configrecord>. The end tag consists of the same name surrounded by angle brackets, but with a forward slash preceding the name, for example </configrecord>. The element content can also contain other "child" elements.

Element Attributes

The XML element attributes that are name-value pairs included in the start tag after the element name. The values must always be quoted, using single or double quotes. Each attribute name should appear only once in an element.

Figure 4-2 shows an XML example which consists of a declaration (first line), nested elements with attributes and content.

Figure 4-2 XML Example

The EDS-MD 4/8/16 wired IoT device gateway uses the attributes in the following subsections to label the group configuration settings.

Record, Group, Item, and Value Tags

A <configgroup> is a logical grouping of configuration parameters and must contain one or more <configitem> elements. It must have a name attribute and may have an instance attribute.

A <configitem> is a specific grouping of configuration parameters relevant to its parent group. An item takes the name attribute and must contain one or more value elements. For example, the line group might have parameters such as baud rate, data bits, and parity.

A value may specify the value of a configuration parameter. It may contain the name attribute. In this example, a value of 9600 might be specified for baud rate; 7 may be specified for data bits, and even may be specified for parity.

A name attribute identifies the group, item, or value. It is always quoted (as are all XML attributes). For example, a group that contains serial port parameters has the name "line".

An instance attribute identifies which of several instances is being addressed. It is always quoted. For example, the serial port name (in the line configgroup) has the instance "1" to indicate serial port 1 or "2" to specify serial port 2.

The following figures show examples of XML configuration records and the use of the <configrecord>, <configroup>, <configitem>, and <value> XML elements.

Figure 4-3 XML Example

Figure 4-4 XML Example of Multiple Named Values

Figure 4-5 XML Example of Multiple Items

```
<configgroup name="ssh server">
      <configitem name="host rsa keys">
        <value name="public key"/>
       <value name="private key"/>
  </configitem>
      <configitem name="host dsa keys">
       <value name="public key"/>
       <value name="private key"/>
  </configitem>
     <configitem name="delete authorized users">
       <value>disable
  </configitem>
      <configitem name="authorized user delete">
       <value name="name"/>
  </configitem>
     <configitem name="authorized user" instance="">
       <value name="password"/>
      <value name="public rsa key"/>
      <value name="public dsa key"/>
  </configitem>
</configgroup>
```

Figure 4-6 XML Example with Multiple Groups

Importing and Exporting an XML Configuration File

An XCR can be imported or exported using the following methods:

- Filesystem-XCRs can be saved to the wired IoT device gateway file system and imported or accessed as needed. See <u>Best Practices on page 19</u> or the Filesystem Browser section in the EDS-MD Wired IoT Device Gateway User Guide.
- CLI-XCRs can be imported (captured) or exported (dumped) directly to a Telnet, SSH, or serial line CLI session. Capturing an XCR can be started by pasting a valid XCR directly into the CLI prompt. The EDS-MD 4/8/16 wired IoT device gateway immediately processes the configuration record, changing any settings specified. This can be done on any level, including the root. Special tags in the XML allow for providing root and enable level passwords so that this can also be done at the password prompt.
- Web browser-Web Manager can be used to import and export an XCR to the wired IoT device gateway file system. It can also be used to import an XCR from an external source such as your local hard drive.
- FTP-The wired IoT device gateway FTP server can export and import XCRs when an FTP get or put command on the filename (edsmd.xcr for export, edsmd_import.xcr for import; both are under the pwxc directory) is requested. On export (FTP get of edsmd.xcr), the FTP server obtains the current XCR from the EDS-MD 4/8/16 wired IoT device gateway and sends it as a file. On import (FTP put of edsmd_import.xcr), the FTP server processes the file by sending it directly to the XML engine. In both cases the wired IoT device gateway filesystem is not accessed. The files edsmd.xcr and edsmd_import.xcr are not read from or written to the file system. See FTP in the EDS-MD Wired IoT Device Gateway User Guide.

Best Practices

You can import or export an entire XCR, or just a portion of it, by specifying the group name and/or group instances. In the examples below, import and export operations are performed from the CLI on the local filesystem and require a XCR on the local filesystem. The Web Manager provides the same functionality.

Caution:

Using Microsoft Word to edit and save an XCR will change the format of the file and make it incompatible with the EDS-MD 4/8/16 wired IoT device gateway. This is true even if the file is saved as Plain Text (.txt) or an XML Document (.xml). Notepad, a third party text editor, or a specialized XML editor should be used instead.

Importing

The following syntax can be used to import configurations from a file:

```
xcr import <file>
xcr import <file> <groups and/or group:instances>
```

The first line imports all groups specified in the XML config record named in <file>. Any filename is valid, and the file name and extension are not important.

In the second line:

- Instance follows group with a colon (see the third example on the next page).
- Multiple groups are separated with a comma.

- Any white space requires the list of groups to be quoted.
- Only the named groups get imported, even if the XCR contains additional XCR groups.

The following syntax can be used to export configurations to a file on the wired IoT device gateway file system:

```
xcr export <file>
xcr export <file> <groups and/or group:instances>
```

The same guidelines above regarding importing configurations also apply to exporting configurations. If no groups are specified, then the export command will export all configuration settings to the file. If instances are specified after the groups, only those group instances are written. If no instance is specified, all instances of that group are written.

Exporting

The following example exports only the accept mode tunneling settings for line 1 to the file "tunnel_1.xcr" on the wired IoT device gateway filesystem:

```
xcr export tunnel 1.xcr "tunnel accept:1"
```

The following example exports only the connect mode tunneling settings for all ports to the file "tunnel_all.xcr" on the wired IoT device gateway filesystem:

```
xcr export tunnel all.xcr "tunnel connect"
```

The following example imports only the settings for line 2 from an XCR named "factory_config.xcr" on the wired IoT device gateway filesystem. If "factory_config.xcr" has other configuration settings, they are ignored:

```
xcr import factory config.xcr "line:2"
```

The following example imports only line settings for all ports from a configuration record on the wired IoT device gateway filesystem named "foobar.xcr":

```
xcr import foobar.xcr "line"
```

To import only disconnect mode tunnel settings for port 1 and all serial line tunnel settings for port 2 from an XML configuration record named "production.xcr" that contains these settings (and possibly more), issue the following command:

```
xcr import production.xcr "tunnel disconnect:1"
```

The following example imports all tunneling settings and line settings for all serial ports from a file named xcr_file:

```
xcr import xcr_file "tunnel accept, tunnel connect, tunnel
disconnect, tunnel modem, tunnel packing, tunnel serial, tunnel
start, tunnel stop, line"
```

The following example exports only accept mode tunneling settings on serial port 1, and line settings on serial port 2 to a file named tunnel_config_t1_l2.xcr on the wired IoT device gateway filesystem.

```
xcr export tunnel config t1 12.xcr "tunnel accept:1, line:2"
```

The following example exports connect mode tunneling and line settings for all ports to the file tunnel_config.xcr on the wired IoT device gateway filesystem:

```
xcr export tunnel config.xcr "tunnel, line"
```

XML Configuration Groups

Table 4-7 lists the EDS-MD 4/8/16 wired IoT device gateway XCR groups in alphabetical order. This table indicates the various group items, as well as some possible value names and options.

Note: Any instance of **<** in the table may be read as "less than" and any instance of **>** may be read as "greater than".

Table 4-7 XCR Groups

Group Name	Group Item	Value Name	Value Options	Additional Information
action:instance ("instance" attribute is "ethN link state change")	delay		N seconds, where N is an integer that represents the delay in seconds	Default: 5 seconds
	email	alarm email	None or Email N where N is an integer between 1 and 16 that represents the email profile number	
		alarm message		
		alarm reminder interval	<none> or N where N is an integer that represents the interval in minutes</none>	Default: <none></none>
		normal email	None or Email N where N is an integer between 1 and 16 that represents the email profile number	
		normal message		
		normal reminder interval	<none> or N where N is an integer that represents the interval in minutes</none>	Default: <none></none>
	ftp put	reminder interval	<none></none>	Default: <none></none>
		mode		Default: Simultaneous
		connection N host		
		connection N port		Default: 21
		connection N filename		Default: data.txt
		connection N protocol		Default: FTP
		connection N username		Default: anonymous
		connection N password		

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
	http post	reminder interval	<none></none>	Default: <none></none>
		mode		Default: Simultaneous
		connection N host		
		connection N port		Default: 80
		connection N url		Default: data.txt
		connection N protocol		Default: HTTP
		connection N username		
		connection N password		
arp	arp delete	ip address		Remove an entry from the ARP table. Specify the entry by its IP address.
	arp entry	ip address		
		mac address		
cli	enable level password			Value is SECRET, hidden from user view.
	inactivity timeout			Default: 15 minutes
	line authentication		enable, disable	Default: disable
	login password			Value is SECRET, hidden from user view. Default: PASS
	quit connect line			Accepts text containing control characters, for example, <control>A represents control-A Default: <control>L</control>
clock	synchronization method	SNTP	SNTP, Manual	
	ntp	server		Default: 0.pool.ntp.org
clock time and zone	time zone	zone		
		offset		Default: +0000 will set the time zone to UTC.
	time set	hours		НН
		minutes		MM
		seconds		SS
		day of month		DD
		month		MM
		year		YYYY
consoleflow	state		enable, disable	Default: disable

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
	device id			
	device key			Value is secret, hidden from user view.
	device name			Default: EDS-MD
	device description			
	status update interval		N minutes	Default: 1 minutes
	content check interval		N hours	Default: 24 hours
	apply firmware upgrade		enable, disable	
	apply configuration updates		Always, Never, If unchanged	
	reboot after update		enable, disable	
	active connection		Connection 1, Connection 2	
	connection: instance ("Instance" attribute is a number.)	host		Default: api.consoleflow.com
		port		Default: 443
		secure port	enable, disable	
		validate certificates	enable, disable	
		mqtt state	enable, disable	
		mqtt host		Default: mqtt.consoleflow.com
		mqtt port		Default: 443
		mqtt security	enable, disable	Default: enable
		use proxy	enable, disable	Default: disable
		proxy type	SOCKS5	
		proxy host		
		proxy port		Default: 80
		proxy username		
		proxy password		
consoleflow line:	state		enable, disable	Default: disable
instance ("Instance" attribute is a	project tag			
number.)	command delimiter			Default: +++
	status update interval		N minutes	Default: 1 minutes
	content check interval		N hours	Default: 24 hours
device	firmware version			Read only.
	long name			
	serial number			Read only.
	short name			

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
dhcp server	state		enable, disable	Default: disable
	start ip address			Default: 192.168.0.20
	end ip address			Default: 192.168.0.254
	lease time			Default: 24 hours
	static leases ("instance" attribute is a number)	mac address		static lease instance can be 1-8
		ip address		Default: <none></none>
diagnostics	log	output	Disable, Filesystem, Line 1-4	Default: disable
		max length		Max size in Kbytes allowed for log.txt
		verbosity level	Minimum, Intermediate, Everything	Default: Minimum
discovery	state		enable, disable	Default: enable
email:instance	СС			
("Instance" attribute is a number.)	message file			
,	priority		urgent, high, normal, low, very low	Default: normal
	from			
	overriding domain			
	local port			
	server port			
	reply to			
	subject			
	to			
ethernet:instance	duplex		auto, half, full	Default: auto
("Instance" attribute is "eth0", "eth1", or "eth2".)	speed		auto, 10, 100	Default: auto
ftp server	state		enable, disable	Default: enable

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
gateway	wan	operating mode	Disabled, Gateway	Default: Disabled
		firewall	enable, disable	
		wan interface	eth0, eth1, eth2	
		router ip address		
		primary dns		Default: <none></none>
		secondary dns		Default: <none></none>
	port forwarding ("instance" attribute is a number)	state	enable, disable	
		friendly name		
		port or range		
		target port		
		protocol	Both, TCP, UDP	Default: Both
		ingress ip address		Default: <none></none>
		ip address		Default: <none></none>
	static routes ("instance" attribute is a number)	state	enable, disable	
		network		
		gateway		
		metric		
		interface	eth0, eth1, eth2	
		friendly name		
host:instance	name			
("Instance" attribute	protocol		telnet, ssh	Default: telnet
is a number.)	ssh username			
	remote address			
	remote port			Default: 0
http authentication uri	user delete	name		Deletes an HTTP Authentication URI user. The value element is used to specify the user for deletion.
	realm			
	type			
	user (instance is "admin")	password		

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
http server	state		enable, disable	Default: enable
	port		<none>,</none>	Default: 80
	secure port		<none>,</none>	Default: 443
	secure protocols		ssl3, tls1.0, tls1.1	May contain zero, one, or more of the values, separated by commas. Default: ssl3, tls1.0, tls1.1
	secure credentials			
	max timeout			Default: 10 seconds
	max bytes			Default: 40960
	logging state		enable, disable	Default: enable
	max log entries			Default: 50
	log format			Default: %h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"
	authentication timeout			Default: 30 minutes
icmp	state		enable, disable	

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
interface: instance	state		enable, disable	
("Instance" attribute	bootp		enable, disable	Default: disable
is "eth0", "eth1", or "eth2")	dhcp		enable, disable	Default: enable
Cuiz)	priority			Accepts a priority between 0 and 10. A lower number signifies a higher preference.
	ip address		<none>,</none>	Accepts an IP address and mask as either: (1) IP address only (192.168.1.1) gets a default mask, (2) CIDR (192.168.1.1/24), or (3) Explicit mask (192.168.1.1 255.255.255.0).
	default gateway		<none>,</none>	Accepts in IP address in dotted notation, like 192.168.1.1.
	hostname			
	domain			
	dhcp client id			
	primary dns		<none>,</none>	Accepts in IP address in dotted notation, like 192.168.1.1.
	secondary dns		<none>,</none>	Accepts in IP address in dotted notation, like 192.168.1.1.
	mtu			Default: 1500 bytes
ip	ip time to live			Default: 64 hops
	multicast time to live			Default: 1 hops
line:instance ("Instance" attribute is a number.)	name			
	state		enable, disable	Default: depends on instance
	protocol		none, tunnel	Default:
	baud rate			Default: 9600 bits per second
	parity		even, none, odd	Default: none
	data bits		7, 8	Default: 8
	stop bits		1, 2	Default: 1
	flow control		none, hardware, software	Default: none

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
	xon char			Accepts a control character, for example, <control>A represents control-A Default: <control>Q</control>
	xoff char			Accepts a control character, for example, <control>A represents control-A Default: <control>S</control>
	gap timer		<none>,</none>	Default: <none></none>
	threshold			Default: 56 bytes
modbus	tcp server state		enable, disable	
	additional port		<none></none>	
	response timeout			
	rss	trace input	enable, disable	
network failover:	state		enable, disable	Default: disable
instance ("instance attribute is eth0,	hostname			
eth1, eth2.)	method		ICMP, TCP	
	timeout			
	interval			
	failover threshold		N pings	
	failback threshold		N pings	
	failover interface			
rss	feed		enable, disable	Default: disable
	persist		enable, disable	Default: disable
	max entries			Default: 100

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
serial command mode: instance	mode		always, serial string, disable	Default: disable
("Instance" attribute is a number.)	echo serial string		enable, disable	Default: enable
is a number.)	serial string			Sets a string that can be entered at boot time to enter command mode. This text may specify binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.
	signon message			Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. This text may specify binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
	wait time			Default: 5000 milliseconds
smtp	relay address			
	relay port			Default: 25
snmp	snmpd	state		
		port		
		version		
		read community		
		write community		
		uername		
		security		
		authentication protocol		
		authentication password		
		privacy protocol		
		privacy password		
		read-only username		
		read-only security		

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
		read-only		
		authentication		
		protocol		
		read-only		
		authentication		
		password		
		read-only privacy		
		protocol		
		read-only privacy		
		password		
		system contact		
		system name		
		system description		
		system location		
	traps	community		
		primary destination port		
		primary destination		
		secondary destination		
		secondary destination port		
		version		
		username		
		security		
		authentication protocol		
		authentication password		
		privacy protocol		
		privacy password		
ssh	state		enable, disable	Default: enable
	port			Default: 22
	max sessions			Default: 3

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
ssh client	delete known hosts		enable, disable	If enabled, deletes any existing hosts before adding "known host".
	known host delete	name		Specify the known host to delete.
	known host	public rsa key		
		public dsa key		
	delete client users		enable, disable	If enabled, deletes any existing client users before adding "client user".
	client user delete	name		Specify the user to delete.
	client user	password		
		remote command		
		public rsa key		
		private rsa key		
		public dsa key		
		private dsa key		
ssh server	host rsa keys	public key		
		private key		
	host dsa keys	public key		
		private key		
	delete authorized users		enable, disable	
	authorized user delete	name		
	authorized user	password		
		public rsa key		
		public dsa key		

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
ssl	credentials	rsa certificate		
		rsa private key type		Value is SECRET, hidden from user view.
		dsa certificate		
	trusted authority ("Instance" attribute is a number)	certificate		
	intermediate authority ("Instance" attribute is a number)	certificate		
	delete all credentials		enable, disable	If enabled, deletes any existing credentials before adding "credentials".
	delete all cas		enable, disable	If enabled, deletes any existing trusted cas before adding "trusted ca".
syslog	state		enable, disable	Default: disable
	host			
	remote port			Default: 514
	severity log level		none, emergency, alert, critical, error, warning, notice, information, debug	Default: none
telnet	state		enable, disable	Default: enable
	port			Default: 23
	max sessions			Default: 3
	authentication		enable, disable	Default: disable
terminal:instance	terminal type			Default: UNKNOWN
("Instance" attribute	login connect menu		enable, disable	Default: disable
is a number or "network")	exit connect menu		enable, disable	Default: disable
,	send break			Accepts a control character, for example, <control>A represents control-A</control>
	break duration			Default: 500 milliseconds
	echo		enable, disable	Default: enable

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
tunnel	accept mode		disable, always	Default: always
accept:instance ("Instance" attribute is a number.)	start character			Accepts a control character, for example, <control>A represents control-A Default: <control>B</control>
	flush start character		enable, disable	Default: enable
	local port			Default: 0
	protocol		tcp, ssh, telnet, tcp aes, ssl	Default: tcp
	credentials			
	tcp keep alive		<none>,</none>	Default: 45000 milliseconds
	aes encrypt key			Value is SECRET, hidden from user view.
	aes decrypt key			Value is SECRET, hidden from user view.
	flush serial		enable, disable	Default: disable
	block serial		enable, disable	Default: disable
	block network		enable, disable	Default: disable
	password	password		Value is SECRET, hidden from user view.
		prompt	enable, disable	Default: disable
	email connect		<none>,</none>	Default: <none></none>
	email disconnect		<none>,</none>	Default: <none></none>

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
tunnel connect:instance ("Instance" attribute is a number.)	connect mode		disable, always, any character, start character, modem control asserted, modem emulation	Default: disable
	start character			Accepts a control character, for example, <control>A represents control-A Default: <control>B</control>
	flush start character		enable, disable	Default: enable
	local port		<random>, </random>	Default: <random></random>
	host	address		
	("Instance" attribute is a number)	port	<none>,</none>	Default: <none></none>
	a namber)	protocol	tcp, udp, ssh, telnet, tcp aes, udp aes, ssl	Default: tcp
		ssh username		
		credentials		
		validate certificate	enable, disable	Default: enable
		tcp keep alive	<none>,</none>	Default: 45000 milliseconds
		aes encrypt key		Value is SECRET, hidden from user view.
		aes decrypt key		Value is SECRET, hidden from user view.
	host mode		sequential, simultaneous	Default: sequential
	reconnect time			Default: 15000 milliseconds
	flush serial		enable, disable	Default: disable
	block serial		enable, disable	Default: disable
	block network		enable, disable	Default: disable
	email connect		<none>,</none>	Default: <none></none>
	email disconnect		<none>,</none>	Default: <none></none>
tunnel disconnect:instance ("Instance" attribute is a number.)	stop character			Accepts a control character, for example, <control>A represents control-A</control>
	flush stop character		enable, disable	Default: enable
	modem control		enable, disable	Default: disable
	timeout			Default: 0 milliseconds
	flush serial		enable, disable	Default: disable

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
tunnel modem:instance ("Instance" attribute is a number.)	echo pluses		enable, disable	Default: disable
	echo commands		enable, disable	Default: enable
	verbose response		enable, disable	Default: enable
	response type		text, numeric	Default: text
	error unknown commands		enable, disable	Default: disable
	incoming connection		disabled, automatic, manual	Default: disabled
	connect string			
	display remote ip		enable, disable	Default: disable
tunnel packing:instance ("Instance" attribute is a number.)	packing mode		disable, timeout, send character	Default: disable
	timeout			Default: 1000 milliseconds
	threshold			Default: 512 bytes
	send character			Accepts a control character, for example, <control>A represents control-A Default: <control> M</control>
	trailing character			Accepts a control character, for example, <control>A represents control-A</control>
tunnel serial:instance ("Instance" attribute is a number.)	dtr		asserted while connected, continuously asserted, unasserted, truport	Default: asserted while connected
xml import control	restore factory configuration		enable, disable	
	delete http authentication uris		enable, disable	Deletes existing HTTP authentication URIs before importing new ones.
	http authentication uri delete	name		Deletes the specified HTTP authentication URI.
	reboot		enable, disable	Reboots after importing.

XML Status Record Groups and Items

Table 4-8 lists the supported XML Status Record (XSR) groups and items. These groups and items show the status of the device in XML form and can only be exported. The XSR schema differs slightly from the XCR groups and items in that the XSR allows groups within groups.

Note: The Valid Values column of Table 4-8 indicates the default value.

Table 4-8 XSR Group and Items

Group Name	Item Name	Value Name	Valid Values
action:instance ("instance" attribute is "ethN link state change")	alarm state		off, on
	duration		duration in N days 00:00:00 (hh:mm:ss)
	transitions		
arp	arp entry	ip address	ip address in format nnn.nnn.nnn.nnn
		mac address	mac address in format xx:xx:xx:xx:xx
		type	dynamic or static
		interface	eth0 or wlan0
clock	time		real time clock time in format hh:mm:ss <timezone></timezone>
	date		real time clock date in format dayofweek day month year
	timezone	zone	
		offset	
consoleflow	serial number		string
	device id		string
	status		Running, Inactive
device	product info	product type	Lantronix EDS-MD
		serial number	12 hex digits
		firmware version	string in version format like 7.3.0.1R7
		uptime	elapsed time in format d days hh:mm:ss
		permanent config	saved or unsaved
email:instance ("Instance" attribute is " <decimal>")</decimal>	success	sent	decimal number
		sent with retries	decimal number
	failed		decimal number
	queued		decimal number
email log:instance ("Instance" attribute is	entry	time	timestamp in format d days hh:mm:ss
" <decimal>")</decimal>		log	string

Group Name (continued)	Item Name	Value Name	Valid Values
failover: instance	state		
("instance" attribute is eth0, eth1, eth2)	transitions		decimal number
hardware	cpu	speed	string
		type	string
	memory	flash size	decimal number
		ram size	decimal number
http	state		
	logging	entries	
		bytes	
http log	totals	entries	decimal number
		bytes	decimal number
	entry ("Instance" attribute is " <decimal>" or number)</decimal>		String
icmp	snmp	InMsgs	decimal number
		InErrors	decimal number
		InDestUnreachs	decimal number
		InTimeExcds	decimal number
		InParmProbs	decimal number
		InSrcQuenchs	decimal number
		InRedirects	decimal number
		InEchos	decimal number
		InEchoReps	decimal number
		InTimestamps	decimal number
		InTimestampReps	decimal number
		InAddrMasks	decimal number
		InAddrMaskReps	decimal number
		OutMsgs	decimal number
		OutErrors	decimal number
		OutDestUnreachs	decimal number
		OutTimeExcds	decimal number
		OutParmProbs	decimal number
		OutSrcQuenchs	decimal number
		OutRedirects	decimal number
		OutEchos	decimal number
		OutEchoReps	decimal number
		OutTimestamps	decimal number
		OutTimestampReps	decimal number
		OutAddrMasks	decimal number
		OutAddrMaskReps	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
interface:instance ("Instance" attribute is "eth0", "eth1", or "eth2")	default gateway	status	dotted notation
	ip address		dotted notation
	generic	status	Link up
	network mask		dotted notation
	receive	bytes	decimal number
		packets	decimal number
		errs	decimal number
		drop	decimal number
		fifo	decimal number
		frame	decimal number
		compressed	decimal number
		multicast	decimal number
	transmit	bytes	decimal number
		packets	decimal number
		errs	decimal number
		drop	decimal number
		fifo	decimal number
		colls	decimal number
		carrier	decimal number
		compressed	decimal number
ip	snmp	Forwarding	decimal number
		DefaultTTL	decimal number
		InReceives	decimal number
		InHdrErrors	decimal number
		InAddrErrors	decimal number
		ForwDatagrams	decimal number
		InUnknownProtos	decimal number
		InDiscards	decimal number
		InDelivers	decimal number
		OutRequests	decimal number
		OutDiscards	decimal number
		OutNoRoutes	decimal number
		ReasmTimeout	decimal number
		ReasmReqds	decimal number
		ReasmOKs	decimal number
		ReasmFails	decimal number
		FragOKs	decimal number
		FragFails	decimal number
		FragCreates	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
ip (continued)	netstat	InNoRoutes	decimal number
		InTruncatedPkts	decimal number
		InMcastPkts	decimal number
		OutMcastPkts	decimal number
		InBcastPkts	decimal number
		OutBcastPkts	decimal number
		InOctets	
		OutOctets	
		InMcastOctets	
		OutMcastOctets	
		InBcastOctets	
		OutBcastOctets	
ip sockets	ip socket	protocol	tcp or udp
		rx queue	decimal number
		tx queue	decimal number
		local address	ip address in format nnn.nnn.nnn
		local port	decimal number
		remote address	ip address in format nnn.nnn.nnn
		remote port	decimal number or *
		state	LISTEN, SYN_RECVD, SYN_SENT, ESTABLISHED, CLOSE_WAIT, LAST_ACK, FIN_WAIT_1, FIN_WAIT_2, CLOSING, or TIME_WAIT.
line:instance ("Instance"	receiver	bytes	decimal number
attribute is " <decimal>")</decimal>		breaks	decimal number
		parity errors	decimal number
		framing errors	decimal number
		overrun errors	decimal number
		no receive buffer errors	decimal number
		queued bytes	decimal number
tı		flow control	go, stop, or n/a
	transmitter	bytes	decimal number
		breaks	decimal number
		queued bytes	decimal number
		flow control	go, stop, or n/a
	line levels	cts input	asserted or not asserted
		rts output	asserted or not asserted
		dsr input	asserted or not asserted
		dtr output	asserted or not asserted

Group Name (continued)	Item Name	Value Name	Valid Values
line (group nested within line above)	state		enable or disable
	protocol		Tunnel or None.
	baud rate		<decimal> bits per second</decimal>
	parity		None, Odd, or Even
	data bits		7 or 8
	stop bits		1 or 2
	flow control		None, Hardware, or Software
	xon char		of form <control> ;Q</control>
	xoff char		of form <control> ;S</control>
memory	main heap	total memory	decimal number of bytes
modbus local slave	totals	pdus in	
		pdus out	
		exceptions	
modbus tcp server	state		
(Attribute of an instance			
includes, "additional" and			
"permanent".)			
	local port		
	totals	uptime	
		pdus in	
		pdus out	
		connections	
	last connection	local ip address	
		local port	
		remote ip address	
		remote port	
processes	process ("Instance" attribute is " <decimal>")</decimal>	stack used	decimal number
	auribute is <decimal>)</decimal>	stack size	decimal number
		cpu %	decimal number
		thread name	String
query port	last connection	ip address	ip address in format nnn.nnn.nnn.nnn
		port	decimal number
	in	discoveries	decimal number
		unknown queries	decimal number
		erroneous packets	decimal number
	out	discovery replies	decimal number
		errors	decimal number
	status	enabled, disabled	

Group Name (continued)	Item Name	Value Name	Valid Values
rss	url		string in the form of a web url
	data	entries	decimal number
		bytes	decimal number
	telnet or ssh ("Instance" attribute is " <number>")</number>	local port	
		remote ip address	
		remote port	
		duration	

Group Name (continued)	Item Name	Value Name	Valid Values
tcp	snmp	RtoAlgorithm	decimal number
	·	RtoMin	decimal number
		RtoMax	decimal number
		MaxConn	decimal number
		ActiveOpens	decimal number
		PassiveOpens	decimal number
		AttemptFails	decimal number
		EstabResets	decimal number
		CurrEstab	decimal number
		InSegs	decimal number
		OutSegs	decimal number
		RetransSegs	decimal number
		InErrs	decimal number
		OutRsts	decimal number
	netstat	SyncookiesSent	decimal number
		SyncookiesRecv	decimal number
		SyncookiesFailed	decimal number
		EmbryonicRsts	decimal number
		PruneCalled	decimal number
		RcvPruned	decimal number
		OfoPruned	decimal number
		OutOfWindowIcmps	decimal number
		LockDroppedIcmps	decimal number
		ArpFilter	decimal number
		TW	decimal number
		TWRecycled	decimal number
		TWKilled	decimal number
		PAWSPassive	decimal number
		PAWSActive	decimal number
		PAWSEstab	decimal number
		DelayedACKs	decimal number
		DelayedACKLocked	decimal number
		DelayedACKLost	decimal number
		ListenOverflows	decimal number
		ListenDrops	decimal number
		TCPPrequeued	decimal number
		TCPDirectCopyFromBacklo g	decimal number
		TCPDirectCopyFromPreque ue	decimal number
		TCPPrequeueDropped	decimal number
	TCPHPHits	decimal number	

Group Name (continued)	Item Name	Value Name	Valid Values
tcp (continued)		TCPHPHitsToUser	decimal number
		TCPPureAcks	decimal number
		TCPHPAcks	decimal number
		TCPRenoRecovery	decimal number
		TCPSackRecovery	decimal number
		TCPSACKReneging	decimal number
		TCPFACKReorder	decimal number
		TCPSACKReorder	decimal number
		TCPRenoReorder	decimal number
		TCPTSReorder	decimal number
		TCPFullUndo	decimal number
		TCPPartialUndo	decimal number
		TCPDSACKUndo	decimal number
		TCPLossUndo	decimal number
		TCPLoss	decimal number
		TCPLostRetransmit	decimal number
		TCPRenoFailures	decimal number
		TCPSackFailures	decimal number
		TCPLossFailures	decimal number
		TCPFastRetrans	decimal number
		TCPForwardRetrans	decimal number
		TCPSlowStartRetrans	decimal number
		TCPTimeouts	decimal number
		TCPRenoRecoveryFail	decimal number
		TCPSackRecoveryFail	decimal number
		TCPSchedulerFailed	decimal number
		TCPRcvCollapsed	decimal number
		TCPDSACKOldSent	decimal number
		TCPDSACKOfoSent	decimal number
		TCPDSACKRecv	decimal number
		TCPDSACKOfoRecv	decimal number
		TCPAbortOnSyn	decimal number
		TCPAbortOnData	decimal number
		TCPAbortOnClose	decimal number
		TCPAbortOnMemory	decimal number
		TCPAbortOnTimeout	decimal number
		TCPAbortOnLinger	decimal number
		TCPAbortFailed	decimal number
		TCPMemoryPressures	decimal number
		TCPSACKDiscard	decimal number
		TCPDSACKIgnoredOld	decimal number
		TCPDSACKIgnoredNoUndo	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
tcp (continued)	netstat (continued)	TCPSpuriousRTOs	decimal number
		TCPMD5NotFound	decimal number
		TCPMD5Unexpected	decimal number
		TCPSackShifted	decimal number
		TCPSackMerged	decimal number
		TCPSackShiftFallback	decimal number
		TCPBacklogDrop	decimal number
		TCPMinTTLDrop	decimal number
		TCPDeferAcceptDrop	decimal number
		IPReversePathFilter	decimal number
		TCPTimeWaitOverflow	decimal number
tunnel:instance ("Instance" attribute is a number.)	aggregate	completed connects	decimal number
		completed accepts	decimal number
		disconnects	decimal number
		dropped connects	decimal number
		dropped accepts	decimal number
		octets from serial	decimal number
		octets from network	decimal number
		connect 0 connection time	elapsed time in format d days hh:mm:ss
		connect 1 connection time	elapsed time in format d days hh:mm:ss
		connect 2 connection time	elapsed time in format d days hh:mm:ss
		connect 3 connection time	elapsed time in format d days hh:mm:ss
		connect 4 connection time	elapsed time in format d days hh:mm:ss
		connect 5 connection time	elapsed time in format d days hh:mm:ss
		connect 6 connection time	elapsed time in format d days hh:mm:ss
		connect 7 connection time	elapsed time in format d days hh:mm:ss
		connect 8 connection time	elapsed time in format d days hh:mm:ss
		connect 9 connection time	elapsed time in format d days hh:mm:ss
		connect 10 connection time	elapsed time in format d days hh:mm:ss
		connect 11 connection time	elapsed time in format d days hh:mm:ss
		connect 12 connection time	elapsed time in format d days hh:mm:ss

Group Name (continued)	Item Name	Value Name	Valid Values
tunnel:instance ("Instance" attribute is a number.) (continued)	aggregate (continued)	connect 13 connection time	elapsed time in format d days hh:mm:ss
,		connect 14 connection time	elapsed time in format d days hh:mm:ss
		connect 15 connection time	elapsed time in format d days hh:mm:ss
		accept connection time	elapsed time in format d days hh:mm:ss
		connect dns address changes	decimal number
		connect dns address invalids	decimal number
tunnel modem (group	echo commands	enable, disable	
nested within tunnel group)	verbose response	enable, disable	
group)	response type		
	error unknown commands	enable, disable	
	incoming connection		
udp	snmp	InDatagrams	decimal number
		NoPorts	decimal number
		InErrors	decimal number
		OutDatagrams	decimal number
		RcvbufErrors	decimal number
		SndbufErrors	decimal number
xsr	out	bytes	decimal number
		lines	decimal number
		elements	decimal number
	errors		decimal number

5: Commands and Levels

Click the level in the tree structure and it will take you to the command list for that level.

- root
 - o enable (enable)
 - configure (config)
 - action (config-action-select)
 - eth1 link state change (config-action:eth1 link state change)
 - email (config-action-email:eth1 link state change)
 - ftp put (config-action-ftp_put:eth1 link state change)
 - connection 1 (config-action-ftp_putconnection:eth1 link state change:1)
 - connection 2 (config-action-ftp_putconnection:eth1 link state change:2)
 - http post (config-action-http_post:eth1 link state change)
 - connection 1 (config-action-http_postconnection:eth1 link state change:1)
 - connection 2 (config-action-http_postconnection:eth1 link state change:2)
 - snmp trap (config-action-snmp_trap:eth1 link state change)
 - eth2 link state change (config-action:eth2 link state change)
 - email (config-action-email:eth2 link state change)
 - ftp put (config-action-ftp_put:eth2 link state change)
 - connection 1 (config-action-ftp_putconnection:eth2 link state change:1)
 - connection 2 (config-action-ftp_putconnection:eth2 link state change:2)
 - http post (config-action-http_post:eth2 link state change)
 - connection 1 (config-action-http_postconnection:eth2 link state change:1)
 - connection 2 (config-action-http_postconnection:eth2 link state change:2)
 - snmp trap (config-action-snmp_trap:eth2 link state change)
 - on scheduled reboot (config-action:on scheduled reboot)
 - email (config-action-email:on scheduled reboot)
 - ftp put (config-action-ftp_put:on scheduled reboot)
 - connection 1 (config-action-ftp_putconnection:on scheduled reboot:1)
 - connection 2 (config-action-ftp_putconnection:on scheduled reboot:2)
 - http post (config-action-http post:on scheduled reboot)
 - connection 1 (config-action-http_postconnection:on scheduled reboot:1)
 - connection 2 (config-action-http_postconnection:on scheduled reboot:2)
 - snmp trap (config-action-snmp trap:on scheduled reboot)
 - arp (config-arp)
 - cli (config-cli)
 - ssh (config-cli-ssh)
 - telnet (config-cli-telnet)
 - clock (config-clock)

- ntp (config-clock-ntp)
- consoleflow (config-consoleflow)
 - connection 1 (config-consoleflow-connection:1)
 - connection 2 (config-consoleflow-connection:2)
 - line 1 (config-consoleflow-line:1)
 - line 2 (config-consoleflow-line:2)
 - line 3 (config-consoleflow-line:3)
 - line 4 (config-consoleflow-line:4)
 - line 5 (config-consoleflow-line:5)
 - line 6 (config-consoleflow-line:6)
 - line 7 (config-consoleflow-line:7)
 - line 8 (config-consoleflow-line:8)
- diagnostics (config-diagnostics)
 - log (config-diagnostics-log)
- discovery (config-discovery)
- ftp (config-ftp)
- gateway (config-gateway)
 - dhcpserver (config-dhcpd)
 - static leases 1 (config-dhcpd-static leases:1)
 - static leases 2 (config-dhcpd-static_leases:2)
 - static leases 3 (config-dhcpd-static_leases:3)
 - static leases 4 (config-dhcpd-static_leases:4)
 - static leases 5 (config-dhcpd-static leases:5)
 - static leases 6 (config-dhcpd-static_leases:6)
 - static leases 7 (config-dhcpd-static_leases:7)
 - static leases 8 (config-dhcpd-static leases:8)
 - port forwarding rule 1 (config-portforwarding:1)
 - port forwarding rule 2 (config-portforwarding:2)
 - port forwarding rule 3 (config-portforwarding:3)
 - port forwarding rule 4 (config-portforwarding:4)
 - port forwarding rule 5 (config-portforwarding:5)
 - port forwarding rule 6 (config-portforwarding:6)
 - port forwarding rule 7 (config-portforwarding:7)
 - port forwarding rule 8 (config-portforwarding:8)
 - static route 1 (config-staticroute:1)
 - static route 2 (config-staticroute:2)
 - static route 3 (config-staticroute:3)
 - static route 4 (config-staticroute:4)
 - static route 5 (config-staticroute:5)
 - static route 6 (config-staticroute:6)
 - static route 7 (config-staticroute:7)
 - static route 8 (config-staticroute:8)
- host 1 (config-host:1)
- host 2 (config-host:2)
- host 3 (config-host:3)
- host 4 (config-host:4)
- host 5 (config-host:5)
- host 6 (config-host:6)
- host 7 (config-host:7)
- host 8 (config-host:8)
- host 9 (config-host:9)
- host 10 (config-host:10)
- host 11 (config-host:11)
- host 12 (config-host:12)
- host 13 (config-host:13)
- host 14 (config-host:14)

- host 15 (config-host:15)
- host 16 (config-host:16)
- host 17 (config-host:17)
- host 18 (config-host:18)
- host 19 (config-host:19)
- host 20 (config-host:20)
- host 21 (config-host:21)
- host 22 (config-host:22)
- host 23 (config-host:23)
- hast 24 (sanfin hast:24)
- host 24 (config-host:24)
- host 25 (config-host:25)
- host 26 (config-host:26)
- host 27 (config-host:27)
- host 28 (config-host:28)
- host 29 (config-host:29)
- host 30 (config-host:30)
- host 31 (config-host:31)
- host 32 (config-host:32)
- http (config-http)
- icmp (config-icmp)
- if 1 (config-if:eth0)
 - link (config-ethernet:eth0)
- if 2 (config-if:eth1)
 - link (config-ethernet:eth1)
- if 3 (config-if:eth2)
 - link (config-ethernet:eth2)
- ip (config-ip)
- rss (config-rss)
- smtp (config-smtp)
- snmp (config-snmp)
 - snmpd (config-snmp-snmpd)
 - traps (config-snmp-traps)
- syslog (config-syslog)
- terminal 1 (config-terminal:1)
- terminal 2 (config-terminal:2)
- terminal 3 (config-terminal:3)
- terminal 4 (config-terminal:4)
- terminal 5 (config-terminal:5)
 terminal 6 (config-terminal:6)
- terminal 7 (config-terminal:7)
- terminal 7 (config terminal:7)
 terminal 8 (config-terminal:8)
- terminal 9 (config-terminal:9)
- terminal 10 (config-terminal:10)
- terminal 11 (config-terminal:11)
- terminal 12 (config-terminal:12)
- terminal 13 (config-terminal:13)
- terminal 14 (config-terminal:14)
- terminal 15 (config-terminal:15)
- terminal 16 (config-terminal:16)
- device (device)
 - reboot schedule (device-reboot-schedule)

terminal network (config-terminal:network)

- dns (dns)
- <u>email 1 (email:1)</u>
- email 2 (email:2)
- email 3 (email:3)

- email 4 (email:4)
- email 5 (email:5)
- email 6 (email:6)
- email 7 (email:7)
- email 8 (email:8)
- email 9 (email:9)
- email 10 (email:10)
- email 11 (email:11)
- email 12 (email:12)
- email 13 (email:13)
- email 14 (email:14)
- email 15 (email:15)
- email 16 (email:16)
- filesystem (filesystem)
- line 1 (line:1)
- line 2 (line:2)
- line 3 (line:3)
- line 4 (line:4)
- line 5 (line:5)
- line 6 (line:6)
- line 7 (line:7)
- line 8 (line:8)
- line 9 (line:9)
- line 10 (line:10)
- line 11 (line:11)
- line 12 (line:12)
- line 13 (line:13)
- line 14 (line:14)
- line 15 (line:15)
- line 16 (line:16)
- ssh (ssh)
 - client (ssh-client)
 - server (ssh-server)
- ssl (ssl)
 - credentials (ssl-credentials)
 - trusted authorities (ssl-auth)
- tunnel 1 (tunnel:1)
 - accept (tunnel-accept:1)
 - password (tunnel-accept-password:1)
 - connect (tunnel-connect:1)
 - host 1 (tunnel-connect-host:1:1)
 - host 2 (tunnel-connect-host:1:2)
 - host 3 (tunnel-connect-host:1:3)
 - host 4 (tunnel-connect-host:1:4)
 host 5 (tunnel-connect-host:1:5)
 - host 6 (tunnel-connect-host:1:6)
 - host 7 (tunnel-connect-host:1:7)
 - host 8 (tunnel-connect-host:1:8)
 - host 9 (tunnel-connect-host:1:9)
 - host 10 (tunnel-connect-host:1:10)
 - host 11 (tunnel-connect-host:1:11)
 - host 12 (tunnel-connect-host:1:12)
 - host 13 (tunnel-connect-host:1:13)
 - host 14 (tunnel-connect-host:1:14)
 - host 15 (tunnel-connect-host:1:15)
 - host 16 (tunnel-connect-host:1:16)

- disconnect (tunnel-disconnect:1)
- modem (tunnel-modem:1)
- packing (tunnel-packing:1)
- serial (tunnel-serial:1)
- tunnel 2 (tunnel:2)
 - accept (tunnel-accept:2)
 - password (tunnel-accept-password:2)
 - connect (tunnel-connect:2)
 - host 1 (tunnel-connect-host:2:1)
 - host 2 (tunnel-connect-host:2:2)
 - host 3 (tunnel-connect-host:2:3)
 - host 4 (tunnel-connect-host:2:4)
 - host 5 (tunnel-connect-host:2:5)
 - host 6 (tunnel-connect-host:2:6)

 - host 7 (tunnel-connect-host:2:7)
 - host 8 (tunnel-connect-host:2:8)
 - host 9 (tunnel-connect-host:2:9)
 - host 10 (tunnel-connect-host:2:10)
 - host 11 (tunnel-connect-host:2:11)
 - host 12 (tunnel-connect-host:2:12)
 - host 13 (tunnel-connect-host:2:13)
 - host 14 (tunnel-connect-host:2:14)
 - host 15 (tunnel-connect-host:2:15)
 - host 16 (tunnel-connect-host:2:16)
 - disconnect (tunnel-disconnect:2)
 - modem (tunnel-modem:2)
 - packing (tunnel-packing:2)
 - serial (tunnel-serial:2)
- tunnel 3 (tunnel:3)
 - accept (tunnel-accept:3)
 - password (tunnel-accept-password:3)
 - connect (tunnel-connect:3)
 - host 1 (tunnel-connect-host:3:1)
 - host 2 (tunnel-connect-host:3:2)
 - host 3 (tunnel-connect-host:3:3)
 - host 4 (tunnel-connect-host:3:4)
 - host 5 (tunnel-connect-host:3:5)
 - host 6 (tunnel-connect-host:3:6)
 - host 7 (tunnel-connect-host:3:7)
 - host 8 (tunnel-connect-host:3:8)
 - host 9 (tunnel-connect-host:3:9)
 - host 10 (tunnel-connect-host:3:10)
 - host 11 (tunnel-connect-host:3:11)
 - host 12 (tunnel-connect-host:3:12)
 - host 13 (tunnel-connect-host:3:13)
 - host 14 (tunnel-connect-host:3:14)
 - host 15 (tunnel-connect-host:3:15)
 - host 16 (tunnel-connect-host:3:16)
 - disconnect (tunnel-disconnect:3)
 - modem (tunnel-modem:3)
 - packing (tunnel-packing:3)
 - serial (tunnel-serial:3)
- tunnel 4 (tunnel:4)
 - accept (tunnel-accept:4)
 - password (tunnel-accept-password:4)
 - connect (tunnel-connect:4)

- host 1 (tunnel-connect-host:4:1)
- host 2 (tunnel-connect-host:4:2)
- host 3 (tunnel-connect-host:4:3)
- host 4 (tunnel-connect-host:4:4)
- host 5 (tunnel-connect-host:4:5)
- host 6 (tunnel-connect-host:4:6)
- host 7 (tunnel-connect-host:4:7)
- host 8 (tunnel-connect-host:4:8)
- host 9 (tunnel-connect-host:4:9)
- host 10 (tunnel-connect-host:4:10)
- host 11 (tunnel-connect-host:4:11)
- host 12 (tunnel-connect-host:4:12)
- host 13 (tunnel-connect-host:4:13)
- host 14 (tunnel-connect-host:4:14)
- host 15 (tunnel-connect-host:4:15)
- host 16 (tunnel-connect-host:4:16)
- disconnect (tunnel-disconnect:4)
- modem (tunnel-modem:4)
- packing (tunnel-packing:4)
- serial (tunnel-serial:4)
- tunnel 5 (tunnel:5)
 - accept (tunnel-accept:5)
 - password (tunnel-accept-password:5)
 - connect (tunnel-connect:5)
 - host 1 (tunnel-connect-host:5:1)
 - host 2 (tunnel-connect-host:5:2)
 - host 3 (tunnel-connect-host:5:3)
 - host 4 (tunnel-connect-host:5:4)
 - host 5 (tunnel-connect-host:5:5)
 - host 6 (tunnel-connect-host:5:6)
 - host 7 (tunnel-connect-host:5:7)
 - host 8 (tunnel-connect-host:5:8)
 - host 9 (tunnel-connect-host:5:9)
 - host 10 (tunnel-connect-host:5:10)
 - host 11 (tunnel-connect-host:5:11)
 - host 12 (tunnel-connect-host:5:12) host 13 (tunnel-connect-host:5:13)

 - host 14 (tunnel-connect-host:5:14) host 15 (tunnel-connect-host:5:15)
 - host 16 (tunnel-connect-host:5:16)
 - disconnect (tunnel-disconnect:5)
 - modem (tunnel-modem:5)
 - packing (tunnel-packing:5)
 - serial (tunnel-serial:5)
- tunnel 6 (tunnel:6)
 - accept (tunnel-accept:6)
 - password (tunnel-accept-password:6)
 - connect (tunnel-connect:6)
 - host 1 (tunnel-connect-host:6:1)
 - host 2 (tunnel-connect-host:6:2)
 - host 3 (tunnel-connect-host:6:3)
 - host 4 (tunnel-connect-host:6:4)
 - host 5 (tunnel-connect-host:6:5)
 - host 6 (tunnel-connect-host:6:6)
 - host 7 (tunnel-connect-host:6:7)
 - host 8 (tunnel-connect-host:6:8)

- host 9 (tunnel-connect-host:6:9)
- host 10 (tunnel-connect-host:6:10)
- host 11 (tunnel-connect-host:6:11)
- host 12 (tunnel-connect-host:6:12)
- host 13 (tunnel-connect-host:6:13)
- host 14 (tunnel-connect-host:6:14)
- host 15 (tunnel-connect-host:6:15)
- host 16 (tunnel-connect-host:6:16)
- disconnect (tunnel-disconnect:6)
- modem (tunnel-modem:6)
- packing (tunnel-packing:6)
- serial (tunnel-serial:6)
- tunnel 7 (tunnel:7)
 - accept (tunnel-accept:7)
 - password (tunnel-accept-password:7)
 - connect (tunnel-connect:7)
 - host 1 (tunnel-connect-host:7:1)
 - host 2 (tunnel-connect-host:7:2)
 - host 3 (tunnel-connect-host:7:3)
 - host 4 (tunnel-connect-host:7:4)
 - host 5 (tunnel-connect-host:7:5)
 - host 6 (tunnel-connect-host:7:6)
 - host 7 (tunnel-connect-host:7:7)
 - host 8 (tunnel-connect-host:7:8)
 - host 9 (tunnel-connect-host:7:9)
 - host 10 (tunnel-connect-host:7:10)
 - host 11 (tunnel-connect-host:7:11)
 - host 12 (tunnel-connect-host:7:12)
 - host 13 (tunnel-connect-host:7:13)
 - host 14 (tunnel-connect-host:7:14)
 - host 15 (tunnel-connect-host:7:15)
 - host 16 (tunnel-connect-host:7:16) disconnect (tunnel-disconnect:7)
 - modem (tunnel-modem:7)
 - packing (tunnel-packing:7)
 - serial (tunnel-serial:7)
- tunnel 8 (tunnel:8)
 - accept (tunnel-accept:8)
 - password (tunnel-accept-password:8)
 - connect (tunnel-connect:8)
 - host 1 (tunnel-connect-host:8:1)
 - host 2 (tunnel-connect-host:8:2)
 - host 3 (tunnel-connect-host:8:3)
 - host 4 (tunnel-connect-host:8:4)
 - host 5 (tunnel-connect-host:8:5)
 - host 6 (tunnel-connect-host:8:6)
 - host 7 (tunnel-connect-host:8:7)
 - host 8 (tunnel-connect-host:8:8)
 - host 9 (tunnel-connect-host:8:9)
 - host 10 (tunnel-connect-host:8:10)
 - host 11 (tunnel-connect-host:8:11) host 12 (tunnel-connect-host:8:12)
 - host 13 (tunnel-connect-host:8:13)
 - host 14 (tunnel-connect-host:8:14)
 - host 15 (tunnel-connect-host:8:15)
 - host 16 (tunnel-connect-host:8:16)

- disconnect (tunnel-disconnect:8)
- modem (tunnel-modem:8)
- packing (tunnel-packing:8)
- serial (tunnel-serial:8)
- tunnel 9 (tunnel:9)
 - accept (tunnel-accept:9)
 - password (tunnel-accept-password:9)
 - connect (tunnel-connect:9)
 - host 1 (tunnel-connect-host:9:1)
 - host 2 (tunnel-connect-host:9:2)
 - host 3 (tunnel-connect-host:9:3)
 - host 4 (tunnel-connect-host:9:4)
 - host 5 (tunnel-connect-host:9:5)
 - host 6 (tunnel-connect-host:9:6)

 - host 7 (tunnel-connect-host:9:7)
 - host 8 (tunnel-connect-host:9:8)
 - host 9 (tunnel-connect-host:9:9)
 - host 10 (tunnel-connect-host:9:10)
 - host 11 (tunnel-connect-host:9:11)
 - host 12 (tunnel-connect-host:9:12)
 - host 13 (tunnel-connect-host:9:13)
 - host 14 (tunnel-connect-host:9:14) host 15 (tunnel-connect-host:9:15)
 - host 16 (tunnel-connect-host:9:16)
 - disconnect (tunnel-disconnect:9)
 - modem (tunnel-modem:9)
 - packing (tunnel-packing:9)
 - serial (tunnel-serial:9)
- tunnel 10 (tunnel:10)
 - accept (tunnel-accept:10)
 - password (tunnel-accept-password:10)
 - connect (tunnel-connect:10)
 - host 1 (tunnel-connect-host:10:1)
 - host 2 (tunnel-connect-host:10:2)
 - host 3 (tunnel-connect-host:10:3)
 - host 4 (tunnel-connect-host:10:4)
 - host 5 (tunnel-connect-host:10:5)
 - host 6 (tunnel-connect-host:10:6)
 - host 7 (tunnel-connect-host:10:7)
 - host 8 (tunnel-connect-host:10:8)
 - host 9 (tunnel-connect-host:10:9)
 - host 10 (tunnel-connect-host:10:10)
 - host 11 (tunnel-connect-host:10:11)
 - host 12 (tunnel-connect-host:10:12)
 - host 13 (tunnel-connect-host:10:13)
 - host 14 (tunnel-connect-host:10:14)
 - host 15 (tunnel-connect-host:10:15)
 - host 16 (tunnel-connect-host:10:16)
 - disconnect (tunnel-disconnect:10)
 - modem (tunnel-modem:10)
 - packing (tunnel-packing:10)
 - serial (tunnel-serial:10)
- tunnel 11 (tunnel:11)
 - accept (tunnel-accept:11)
 - password (tunnel-accept-password:11)
 - connect (tunnel-connect:11)

- host 1 (tunnel-connect-host:11:1)
- host 2 (tunnel-connect-host:11:2)
- host 3 (tunnel-connect-host:11:3)
- host 4 (tunnel-connect-host:11:4)
- host 5 (tunnel-connect-host:11:5)
- host 6 (tunnel-connect-host:11:6)
- host 7 (tunnel-connect-host:11:7)
- host 8 (tunnel-connect-host:11:8)
- host 9 (tunnel-connect-host:11:9)
- host 10 (tunnel-connect-host:11:10)
- host 11 (tunnel-connect-host:11:11)
- host 12 (tunnel-connect-host:11:12)
- host 13 (tunnel-connect-host:11:13)
- host 14 (tunnel-connect-host:11:14)
- host 15 (tunnel-connect-host:11:15)
- host 16 (tunnel-connect-host:11:16)
- disconnect (tunnel-disconnect:11)
- modem (tunnel-modem:11)
- packing (tunnel-packing:11)
- serial (tunnel-serial:11)
- tunnel 12 (tunnel:12)
 - accept (tunnel-accept:12)
 - password (tunnel-accept-password:12)
 - connect (tunnel-connect:12)
 - host 1 (tunnel-connect-host:12:1)
 - host 2 (tunnel-connect-host:12:2)
 - host 3 (tunnel-connect-host:12:3)
 - host 4 (tunnel-connect-host:12:4)
 - host 5 (tunnel-connect-host:12:5)
 - host 6 (tunnel-connect-host:12:6) host 7 (tunnel-connect-host:12:7)
 - host 8 (tunnel-connect-host:12:8)
 - host 9 (tunnel-connect-host:12:9)

 - host 10 (tunnel-connect-host:12:10) host 11 (tunnel-connect-host:12:11)
 - host 12 (tunnel-connect-host:12:12)
 - host 13 (tunnel-connect-host:12:13)

 - host 14 (tunnel-connect-host:12:14) host 15 (tunnel-connect-host:12:15)
 - host 16 (tunnel-connect-host:12:16)
 - disconnect (tunnel-disconnect:12)
 - modem (tunnel-modem:12)
 - packing (tunnel-packing:12)
 - serial (tunnel-serial:12)
- tunnel 13 (tunnel:13)
 - accept (tunnel-accept:13)
 - password (tunnel-accept-password:13)
 - connect (tunnel-connect:13)
 - host 1 (tunnel-connect-host:13:1)
 - host 2 (tunnel-connect-host:13:2)
 - host 3 (tunnel-connect-host:13:3)
 - host 4 (tunnel-connect-host:13:4)
 - host 5 (tunnel-connect-host:13:5)
 - host 6 (tunnel-connect-host:13:6)
 - host 7 (tunnel-connect-host:13:7)
 - host 8 (tunnel-connect-host:13:8)

- host 9 (tunnel-connect-host:13:9)
- host 10 (tunnel-connect-host:13:10)
- host 11 (tunnel-connect-host:13:11)
- host 12 (tunnel-connect-host:13:12)
- host 13 (tunnel-connect-host:13:13)
- host 14 (tunnel-connect-host:13:14)
- host 15 (tunnel-connect-host:13:15)
- host 16 (tunnel-connect-host:13:16)
- disconnect (tunnel-disconnect:13)
- modem (tunnel-modem:13)
- packing (tunnel-packing:13)
- serial (tunnel-serial:13)
- tunnel 14 (tunnel:14)
 - accept (tunnel-accept:14)
 - password (tunnel-accept-password:14)
 - connect (tunnel-connect:14)
 - host 1 (tunnel-connect-host:14:1)
 - host 2 (tunnel-connect-host:14:2)
 - host 3 (tunnel-connect-host:14:3)
 - host 4 (tunnel-connect-host:14:4)
 - host 5 (tunnel-connect-host:14:5)
 - host 6 (tunnel-connect-host:14:6)
 - host 7 (tunnel-connect-host:14:7)
 - host 8 (tunnel-connect-host:14:8)
 - host 9 (tunnel-connect-host:14:9)
 - host 10 (tunnel-connect-host:14:10)
 - host 11 (tunnel-connect-host:14:11)
 - host 12 (tunnel-connect-host:14:12)
 - host 13 (tunnel-connect-host:14:13)
 host 14 (tunnel-connect-host:14:14)
 - host 15 (tunnel-connect-host:14:15)
 - host 16 (tunnel-connect-host:14:16)
 - disconnect (tunnel-disconnect:14)
 - modem (tunnel-modem:14)
 - packing (tunnel-packing:14)
 - serial (tunnel-serial:14)
- tunnel 15 (tunnel:15)
 - accept (tunnel-accept:15)
 - password (tunnel-accept-password:15)
 - connect (tunnel-connect:15)
 - host 1 (tunnel-connect-host:15:1)
 - host 2 (tunnel-connect-host:15:2)
 - host 3 (tunnel-connect-host:15:3)
 - host 4 (tunnel-connect-host:15:4)
 host 5 (tunnel-connect-host:15:5)
 - host 6 (tunnel-connect-host:15:6)
 - host 7 (tunnel-connect-host:15:7)
 - host 8 (tunnel-connect-host:15:8)
 - host 9 (tunnel-connect-host:15:9)
 - host 10 (tunnel-connect-host:15:10)
 - host 11 (tunnel-connect-host:15:11)
 - host 12 (tunnel-connect-host:15:12)
 - host 13 (tunnel-connect-host:15:13)
 - host 14 (tunnel-connect-host:15:14)
 - host 15 (tunnel-connect-host:15:15)
 - host 16 (tunnel-connect-host:15:16)

- disconnect (tunnel-disconnect:15)
- modem (tunnel-modem:15)
- packing (tunnel-packing:15)
- serial (tunnel-serial:15)
- tunnel 16 (tunnel:16)
 - accept (tunnel-accept:16)
 - password (tunnel-accept-password:16)
 - connect (tunnel-connect:16)
 - host 1 (tunnel-connect-host:16:1)
 - host 2 (tunnel-connect-host:16:2)
 - host 3 (tunnel-connect-host:16:3)
 - host 4 (tunnel-connect-host:16:4)
 - host 5 (tunnel-connect-host:16:5)
 - host 6 (tunnel-connect-host:16:6)
 - host 7 (tunnel-connect-host:16:7)
 - host 8 (tunnel-connect-host:16:8)
 - host 9 (tunnel-connect-host:16:9)
 - host 10 (tunnel-connect-host:16:10)
 - host 11 (tunnel-connect-host:16:11)
 - host 12 (tunnel-connect-host:16:12)
 - host 13 (tunnel-connect-host:16:13)
 - host 14 (tunnel-connect-host:16:14)
 - host 15 (tunnel-connect-host:16:15)

 - host 16 (tunnel-connect-host:16:16)
 - disconnect (tunnel-disconnect:16)
 - modem (tunnel-modem:16)
 - packing (tunnel-packing:16)
 - serial (tunnel-serial:16)
- xml (xml)

accept (tunnel-accept:16) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < <i>number</i> >	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.

initial send binary sinary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the

	initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:15) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.

credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary binary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.

Uses SSL protocol for accept mode tunneling. Uses TCP protocol for accept mode tunneling. Uses TCP protocol with AES encryption for accept mode tunneling. Uses Telnet protocol (with IAC) for accept mode tunneling. Disables the protocol. Enables the protocol.
Uses TCP protocol with AES encryption for accept mode tunneling. Uses Telnet protocol (with IAC) for accept mode tunneling. Disables the protocol. Enables the protocol.
tunneling. Disables the protocol. Enables the protocol.
Enables the protocol.
·
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
Displays tunnel accept status.
Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
Stores the current configuration in permanent memory.
Enables the tunneling server to always accept tunneling connections.
Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
Disables accept mode tunneling.
Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
Enables modem emulation for accept mode tunneling.
Enables accept mode tunneling when the configured start character is received on the line.
Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent

	hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number >	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode

flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary sinary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A</control>

	decimal value character has the form \99. A hex value character has the form 0xFF.
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:13) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).

Forwards (tunnels) serial data in accept mode tunneling.
Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL server.
Restores the default accept mode as "always".
Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the accept mode start character.
Defaults the TCP keep alive idle time.
Restores the default 45 second accept mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
Returns to the tunnel level.
Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
Flushes the serial data buffer upon establishing an accept mode tunneling connection.
Enables forwarding of the accept start character into the network.
Disables forwarding of the accept start character into the network.
Sets the accept tunnel Initial Send text allowing for
binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to
that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>
that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Disconnects the active accept mode tunneling</text>
that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Disconnects the active accept mode tunneling connection. Sets the port to use for accept mode tunneling.</text>
that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Disconnects the active accept mode tunneling connection. Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number></text>

no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:12) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
	Enables the tunneling server to accept tunneling
accept mode any character	connections only when a character is received through the corresponding line (serial port).

accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.

email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
	Sets an email profile to use to send an email alert
email disconnect < number >	upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
	Characters already in the serial data buffer are
flush serial disable	retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary <binary></binary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
5554.5 protocolo (101.12 diodolo	Sissano ino protocon

secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:11) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection.		
block network enable block network enable block network enable block serial disable block serial disable block serial disable block serial disable Forwards (tunnels) serial data in accept mode tunneling. Discards all data coming in from the serial interface (generally used for debugging). Forwards (tunnels) serial data in accept mode tunneling. Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging). clears the screen. Selects the RSA/DSA certificates by name for the SSL server. default accept mode Restores the default accept mode as "always". Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default local port Restores the default protocol as "TCP". default secure protocols default secure protocols Restores the default secure protocol selections. default tart character default top keep alive idle time Defaults the accept mode start character. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. Anumber> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. Anumber> = the number of the email profile to use. Sets an email profile to use. Flushs serial disable flush serial enable flush start character disable flush start character disable flush start character disable flush start character enable initial send binary binary> Sets an eaccept mode tunneling connection. Viritin [] use binary decimal up to 255 or hex up to OxFF. Sets the accept tunnel Initial Send text. Sets on the accept tunnel not on connection. Viritin [] use binary decimal up to 255 or hex up to OxFF. Sets the accept tunnel Initial Send text. Sets i	aes encrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
block network enable tunnel before forwarding it to the serial interface (generally used for debugging). Forwards (tunnels) serial data in accept mode tunneling. Discards all data coming in from the serial interface before forwarding it to the accept mode tunneling. Clars the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL server. default accept mode Restores the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default local port Restores the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default secure protocol Restores the default secure protocol selections. default start character default top keep alive idle time Defaults the accept mode start character. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive inneut. default top keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel connection. Flush serial data buffer upon establishing an accept mode tunneling connection. Flush serial enable Flush start character disable Flush start character disable Enables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text a</number></number></number></number>	block network disable	
block serial disable Discards all data coming in from the serial interface block serial enable Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging). Clears the screen.	block network enable	tunnel before forwarding it to the serial interface (generally used for debugging).
block serial enable before forwarding it to the accept mode tunnel (generally used for debugging). Clears the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL server. default accept mode Restores the default accept mode as "always". Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default start character Defaults the accept mode start character. Defaults the accept mode start character. default top keep alive idle time Restores the default 45 second accept mode TCP keep alive imeout. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. flush serial enable Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Sets the accept tunnel lnitial Send text allowing for binary characters. Sets the accept tunnel lnitial Send text allowing for binary characters. Sets the accept tunnel lnitial Send text. <text> = accident tunnel lnitial Send text. Sets the accept tunnel lnitial Send text. <</text></number></number>	block serial disable	· · · · · · · · · · · · · · · · · · ·
Selects the RSA/DSA certificates by name for the SSL server. default accept mode Restores the default accept mode as "always". Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default protocol Restores the default protocol as "TCP". Restores the default protocol as PTCP". Restores the default secure protocol selections. default start character Defaults the accept mode start character. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive interval default top keep alive interval default top keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email allert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. flush serial enable flush start character disable Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary benary be</number></number>	block serial enable	before forwarding it to the accept mode tunnel (generally used for debugging).
default accept mode Restores the default accept mode as "always". Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections. Defaults serve protocols ledetons. Defaults the accept mode start character. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive imeout. Restores the default 45 second accept mode TCP keep alive timeout. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flush serial enable Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel linitial Send text allowing for binary characters. Sets the accept tunnel linitial Send text allowing for binary characters. Sets the accept tunnel linitial Send text allowing for binary characters. Sets the accept tunnel linitial Send text. <text> = accii string that will be sent out the network upon connection.</text></number></number>	clrscrn	Clears the screen.
Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. default protocol default secure protocols default secure protocol selections. Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive interval default top keep alive interval default top keep alive interval default top keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushs serial enable flush serial enable flush start character disable flush start character disable flush start character disable flush start character enable Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number>	credentials <text></text>	
default local port default protocol default protocol default secure protocols Restores the default protocol as "TCP". Restores the default secure protocol selections. default start character default start character default top keep alive idle time default top keep alive interval default top keep alive interval default top keep alive interval default top keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunnel tunneling connection. Flush serial enable flush start character disable flush start character disable flush start character enable flush start character e</number></number>	default accept mode	Restores the default accept mode as "always".
default secure protocols default start character default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive idle time. Pestores the default searcept mode tunnel TCP keep alive interval default tcp keep al	default local port	accept mode tunneling. The default port is 10000 +
default start character default top keep alive idle time default top keep alive interval default top keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. Sets the accept tunnel Initial Send text allowing for binary characters. Virthin [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number></number>	default protocol	Restores the default protocol as "TCP".
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. <bn></bn> binary characters. <bn></bn> binary characters. <bn></bn> binary characters. <bn></bn> binary binary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number>	·	·
default tcp keep alive interval default tcp keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. flush serial enable Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number></number>		·
default tcp keep alive interval default tcp keep alive probes Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Disables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number></number>	default tcp keep alive idle time	·
Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. exit Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. flush serial enable Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number></number>	default tcp keep alive interval	·
email connect <number> upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. exit Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. flush serial enable flush start character disable flush start character disable flush start character enable flush start character disable flu</number></number></number>	default tcp keep alive probes	Defaults the TCP keep alive probes.
email disconnect <number> email disconnect <number> upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. flush serial enable flush start character disable flush start character disable flush start character enable Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text></number></number></number>	email connect < number >	upon establishing an accept mode tunnel.
Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. Initial send binary Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>	email disconnect < number>	upon closing an accept mode tunnel. <number> =</number>
flush serial disable retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>	exit	Returns to the tunnel level.
accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. binary characters. within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>	flush serial disable	retained upon establishing an accept mode
the network. Disables forwarding of the accept start character into the network. Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. binary characters. binary characters out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>	flush serial enable	
into the network. Sets the accept tunnel Initial Send text allowing for binary characters. sinitial send binary binary > binary > binary > binary > binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>	flush start character disable	Enables forwarding of the accept start character into the network.
binary characters. binary characters. binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon</text>	flush start character enable	
initial send set <text> ascii string that will be sent out the network upon</text>	initial send binary sinary >	binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to</binary>
	initial send set <text></text>	ascii string that will be sent out the network upon

kill connection	Disconnects the active accept mode tunneling connection.
local port < <i>number</i> >	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.

accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
defectly protected	Restores the default protocol as "TCP".
default protocol	restores the deladit protocol as TOI.

default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary sinary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <pre><number> = number of the port to use.</number></pre>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.

secure protocols tls1.0 disable	Disables the protocol.
secure protocols tis1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:9) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary hinary>	Sets the accept tunnel Initial Send text allowing for binary characters. <pre></pre>

	that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:8) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".

default local port default protocol default secure protocols default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number> exit flush serial disable flush start character disable flush start character enable	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. Restores the default protocol as "TCP". Restores the default secure protocol selections. Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network. Disables forwarding of the accept start character</number></number>
default secure protocols default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Restores the default secure protocol selections. Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
default tcp keep alive interval default tcp keep alive probes email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
default tcp keep alive probes email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
email connect <number> email disconnect <number> exit flush serial disable flush start character disable flush start character enable</number></number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number></number>
email disconnect <number> exit flush serial disable flush serial enable flush start character disable flush start character enable</number>	upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.</number>
flush serial disable flush serial enable flush start character disable flush start character enable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.
flush serial disable flush serial enable flush start character disable flush start character enable	retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an accept mode tunneling connection. Enables forwarding of the accept start character into the network.
flush start character disable flush start character enable	accept mode tunneling connection. Enables forwarding of the accept start character into the network.
flush start character enable	the network.
ilush start character enable	Disables forwarding of the accept start character
	into the network.
initial send binary binary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
KIII CODDACTIOD	Disconnects the active accept mode tunneling connection.
	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
., .	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
	Discontinues sending email alerts upon establishing an accept mode tunnel.
no amail disconnact	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
	Uses SSL protocol for accept mode tunneling.
•	Uses TCP protocol for accept mode tunneling.

protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:7) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < <i>number</i> >	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
DVII	
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection. Flushes the serial data buffer upon establishing an

flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary <binary></binary>	Sets the accept tunnel Initial Send text allowing for binary characters. binary characters. binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port < number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
	Sets the accept mode start character. The character
start character <control></control>	may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:6) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.

block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < <i>number</i> >	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary < <i>binary</i> >	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port < <i>number</i> >	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.

no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:5) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.

accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>

email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary binary>	Sets the accept tunnel Initial Send text allowing for binary characters. stinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <pre><number> = number of the port to use.</number></pre>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:4) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value
	if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary binary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

kill connection	Disconnects the active accept mode tunneling connection.
local port < <i>number</i> >	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre></pre>
write	Stores the current configuration in permanent memory.

default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary sinary >	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.

Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Displays the current configuration. Displays the last 20 commands entered during the
current CLI session.
Displays tunnel accept status.
Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
Stores the current configuration in permanent memory.
Enables the tunneling server to always accept tunneling connections.
Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
Disables accept mode tunneling.
Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
Enables modem emulation for accept mode tunneling.
Enables accept mode tunneling when the configured start character is received on the line.
Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default start character	Defaults the accept mode start character.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second accept mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
email connect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary hinary>	Sets the accept tunnel Initial Send text allowing for binary characters. string in binary format

	that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.</number>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:1) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".

default local port default protocol default secure protocols default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number>	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel. Restores the default protocol as "TCP". Restores the default secure protocol selections. Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use. Returns to the tunnel level.</number></number>
default secure protocols default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number>	Restores the default secure protocol selections. Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
default start character default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number>	Defaults the accept mode start character. Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number>	Defaults the TCP keep alive idle time. Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number>	Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
default tcp keep alive interval default tcp keep alive probes email connect < number> email disconnect < number>	Restores the default 45 second accept mode TCP keep alive timeout. Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
email connect < number> email disconnect < number>	Defaults the TCP keep alive probes. Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
email connect < number> email disconnect < number>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use. Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number></number>
	upon closing an accept mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
initial send binary <binary></binary>	Sets the accept tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the accept tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling. <pre><number> = number of the port to use.</number></pre>
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no initial send	Removes the accept tunnel Initial Send string.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.

protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <control></control>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the value for timeouts subsequent to the initial timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
write	Stores the current configuration in permanent memory.
action (config-action-select) level command	ls
clrscrn	Clears the screen.
eth0 link state change	Enters the eth0 link state change alarm level.
eth1 link state change	Enters the eth1 link state change alarm level.
eth2 link state change	Enters the eth2 link state change alarm level.
exit	Exits to the config level.
show history	
Onow motory	Displays the last 20 commands entered during the current CLI session.
write	Displays the last 20 commands entered during the
	Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent
write	Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent
write arp (config-arp) level commands	Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. Adds an entry to the ARP table, mapping an IP address to a MAC address. <ip address=""> = IP address to be mapped. <mac address=""> = MAC</mac></ip>

remove all	Removes all entries from the ARP cache.
remove ip <ip address=""></ip>	Removes an entry from the ARP cache. <ip address=""> = address of the entry being removed.</ip>
show cache	Displays the ARP cache table.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
cli (config-cli) level commands	
clrscrn	Clears the screen.
default inactivity timeout	The default inactivity timeout will apply to CLI sessions.
default login password	Restores the default CLI login password.
default quit connect line	Restores the default string to quit the "connect line", "telnet", and "ssh" commands.
enable level password <text></text>	Sets the enable-level password.
exit	Exits to the configuration level.
inactivity timeout <minutes></minutes>	Sets the inactivity timeout for all CLI sessions.
line authentication disable	No password required for Line CLI users.
line authentication enable	Challenges the Line CLI user with a password.
login password <text></text>	Sets the CLI login password.
no enable level password	Removes the enable-level password.
no inactivity timeout	No inactivity timeout will apply to CLI sessions.
quit connect line <control></control>	Sets the string used to quit the "connect line", "telnet", and "ssh" commands. The characters may be input as text or control. A control character has the form <control>C.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh	Change to menu level for SSH configuration and status.
telnet	Change to menu level for Telnet configuration and status.
write	Stores the current configuration in permanent memory.
client (ssh-client) level commands	
clrscrn	Clears the screen.
default user <username> command</username>	Restore the user command to the default login shell
delete all known hosts	Remove all known hosts
delete all users	Remove all users
delete known host <server></server>	Remove known host
delete user <username></username>	Delete the named user
exit	Exits to the ssh level.
known host <server></server>	Set known host RSA or DSA key
no known host <server> dsa</server>	Remove known host DSA key
no known host <server> rsa</server>	Remove known host RSA key
no user <username> dsa</username>	Remove user DSA key

Remove user RSA key
Show SSH Client settings
Displays the last 20 commands entered during the current CLI session.
Show known host RSA and DSA keys
Show information for a user
Set username and RSA or DSA keys
Customizes the user command
Generate DSA public and private keys
Generate DSA public and private keys
Generate DSA public and private keys
Generate RSA public and private keys
Generate RSA public and private keys
Generate RSA public and private keys
Set username with password and optional RSA or DSA keys
Stores the current configuration in permanent memory.
Sets the system clock.
Shows possible time zone names.
Sets the timezone to be displayed. Use "clock timezone" to show choices.
Clears the screen.
Restores the default timezone, which is UTC.
Restores the default time synchronization method (Manual).
Exits to the configuration level.
Enters the next lower level.
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
Displays the system clock.
Set time manually.
Synchronize time with a NTP server.
Stores the current configuration in permanent memory.
Enters the config action level.
Changes to the command level for ARP configuration and status.
Change to menu level for CLI configuration and status
Change to menu level for Clock configuration and status
_

diagnostics	Enters the diagnostics level.
discovery	Enters the discovery level.
exit	Exits to the enable level.
ftp	Enters the ftp level.
gateway	Enters the gateway level.
host <number></number>	Change to config host level
http	Enters the http level.
icmp	Changes to the command level for ICMP configuration and status.
if <instance></instance>	Changes to the interface configuration level.
ip	Changes to the command level for IP configuration and status.
kill ssh <session></session>	Kills SSH session with index from "show sessions"
kill telnet <session></session>	Kills Telnet session with index from "show sessions"
rss	Change to menu level for RSS configuration and status
show	Displays system information.
show history	Displays the last 20 commands entered during the current CLI session.
show lines	Displays line information.
smtp	Changes to the command level for SMTP configuration and status.
snmp	Enters snmp level.
syslog	Enters the syslog level.
terminal <line></line>	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
write	Stores the current configuration in permanent memory.

connect (tunnel-connect:16) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.

connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host < number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:15) level command	ds
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.

flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <pre><number> = the number of the port to use.</number></pre>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:14) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
	Forwards (tunnels) serial data in connect mode

block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
cirscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>

no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host < number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

connect (tunnel-connect:13) level command	S
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.

default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port < <i>number</i> >	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character < control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

write	Stores the current configuration in permanent memory.
connect (tunnel-connect:12) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.

host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:11) level comm	ands
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface
Sider deliai dilabid	before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	
	(generally used for debugging).
clrscrn	(generally used for debugging). Clears the screen. Enables the tunneling server to always establish

connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port < number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>

show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

connect (tunnel-connect:10) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < <i>number</i> >	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < <i>number</i> >	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.

flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <pre><number> = the number of the port to use.</number></pre>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:9) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.

block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
cirscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>

no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:8) level commands	3
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
	Enables connect mode tunneling when the

default connect mode

default host mode

Restores the default connect mode as "disable".

connection.

Connects to the first host in the list that accepts the

default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port < <i>number</i> >	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character < control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

write	Stores the current configuration in permanent memory.
connect (tunnel-connect:7) level command	ls .
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.

host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <pre><number> = the number of the port to use.</number></pre>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host < number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character < control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:6) level comma	ands
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.

connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port < number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>

show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

connect (tunnel-connect:5) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.

flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:4) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.

block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>

no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:3) level commands	5
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.

default connect mode

default host mode

Restores the default connect mode as "disable".

connection.

Connects to the first host in the list that accepts the

default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

write	Stores the current configuration in permanent memory.
connect (tunnel-connect:2) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.

host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <number></number>	Sets a specific port for use as the local port. <pre><number> = the number of the port to use.</number></pre>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character < control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:1) level comma	ands
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.

connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect < number>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.</number>
email disconnect < number>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.</number>
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port < number>	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <number></number>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>

show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

connection 1 (config-consoleflow-connection:1)	level commands
clrscrn	Clears the screen.
default host	Restores the Hostname or IP address of ConsoleFlow.
default mqtt host	Restores the Hostname or IP address of MQTT server.
default mqtt port	Restores the Port of MQTT server.
default port	Restores the Port of ConsoleFlow.
default proxy port	Restores the Port of proxy server.
default proxy type	Restores the default Proxy server type (SOCKS5).
exit	Exits to the next higher level.
host <text></text>	Sets the Hostname or IP address of ConsoleFlow.
mqtt host <text></text>	Sets the Hostname or IP address of MQTT server.
mqtt port <number></number>	Sets the Port of MQTT server.
mqtt security disable	Disables SSL for MQTT.
mqtt security enable	Enables SSL for MQTT.
mqtt state disable	Disables MQTT.
mqtt state enable	Enables MQTT.
no proxy host	Restores the Hostname or IP address of the proxy server.
no proxy password	Restores the password for proxy server.
no proxy username	Clears the user name for the proxy server.
port <number></number>	Sets the Port of ConsoleFlow.
proxy host <text></text>	Sets the Hostname or IP address of the proxy server.
proxy password <text></text>	Sets the password the proxy server.
proxy port <number></number>	Sets the Port of the proxy server.
proxy type socks5	Sets the Proxy server type to SOCKS5
proxy username <text></text>	Sets the user name for the proxy server.
secure port disable	Disables https for ConsoleFlow client.
secure port enable	Enables https for ConsoleFlow client.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
use proxy disable	Disables use of proxy server for this connection.
use proxy enable	Enables use of proxy server for this connection.
validate certificates disable	Disables certificate validation for ConsoleFlow client.

validate certificates enable	Enables certificate validation for ConsoleFlow client.
write	Stores the current configuration in permanent
	memory.

	, ,
connection 1 (config-action-http_	post-connection:on scheduled reboot:1) level commands
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.
host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port <number></number>	Sets the Port number which HTTP server is listening to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.
write	Stores the current configuration in permanent memory.

connection 1 (config-action-ftp_put-co	onnection:on scheduled reboot:1) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port <number></number>	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.

write	Stores the current configuration in permanent memory.
connection 1 (config-action-http_post-connection	n:eth2 link state change:1) level commands
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.
host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port <number></number>	Sets the Port number which HTTP server is listening to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.

connection 1 (config-action-ftp_pu	t-connection:eth2 link state change:1) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port <number></number>	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.

memory.

Stores the current configuration in permanent

write

write	Stores the current configuration in permanent memory.
connection 1 (config-action-http_post-connection	n:eth1 link state change:1) level commands
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.
host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port <number></number>	Sets the Port number which HTTP server is listening to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.
write	Stores the current configuration in permanent memory.

connection 1 (config-action-ftp_I	put-connection:eth1 link state change:1) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port < <i>number</i> >	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.

write	Stores the current configuration in permanent memory.
connection 2 (config-consoleflow-con	nnection:2) level commands
clrscrn	Clears the screen.
default host	Restores the Hostname or IP address of ConsoleFlow.
default mqtt host	Restores the Hostname or IP address of MQTT server.
default mqtt port	Restores the Port of MQTT server.
default port	Restores the Port of ConsoleFlow.
default proxy port	Restores the Port of proxy server.
default proxy type	Restores the default Proxy server type (SOCKS5).
exit	Exits to the next higher level.
host <text></text>	Sets the Hostname or IP address of ConsoleFlow.
mqtt host <text></text>	Sets the Hostname or IP address of MQTT server.
mqtt port <number></number>	Sets the Port of MQTT server.
mqtt security disable	Disables SSL for MQTT.
mqtt security enable	Enables SSL for MQTT.
mqtt state disable	Disables MQTT.
mqtt state enable	Enables MQTT.
no proxy host	Restores the Hostname or IP address of the proxy server.
no proxy password	Restores the password for proxy server.
no proxy username	Clears the user name for the proxy server.
port <number></number>	Sets the Port of ConsoleFlow.
proxy host <text></text>	Sets the Hostname or IP address of the proxy server.
proxy password <text></text>	Sets the password the proxy server.
proxy port <number></number>	Sets the Port of the proxy server.
proxy type socks5	Sets the Proxy server type to SOCKS5
proxy username <text></text>	Sets the user name for the proxy server.
secure port disable	Disables https for ConsoleFlow client.
secure port enable	Enables https for ConsoleFlow client.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
use proxy disable	Disables use of proxy server for this connection.
use proxy enable	Enables use of proxy server for this connection.
validate certificates disable	Disables certificate validation for ConsoleFlow client.
validate certificates enable	Enables certificate validation for ConsoleFlow client.
write	Stores the current configuration in permanent memory.
connection 1 (config-action-http_pos	t-connection:eth0 link state change:1) level commands
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.
OAIL	EARS TO THE HEALTHIGHT IEVEL.

host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port <number></number>	Sets the Port number which HTTP server is listening to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.
write	Stores the current configuration in permanent memory.

connection 1 (config-action-ftp_put-connection:	eth0 link state change:1) level commands
cirscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port <number></number>	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.
write	Stores the current configuration in permanent memory.

connection 2 (config-action-http_post-connection:on scheduled reboot:2) level commands	
clrscrn Clears the screen.	
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.

host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port <number></number>	Sets the Port number which HTTP server is listening to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.
write	Stores the current configuration in permanent memory.

connection 2 (config-action-ftp_put-connection:	on scheduled reboot:2) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port <number></number>	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.
write	Stores the current configuration in permanent memory.

connection 2 (config-action-http_post-connection:eth2 link state change:2) level commands	
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.

Sets HTTP server IP address or hostname to be connected to.
Clears HTTP server IP address or hostname.
Clears the Password.
Clears HTTP request URL.
Clears the Username.
Sets the Password used to logon to HTTP server.
Sets the Port number which HTTP server is listening to.
Selects HTTP Protocol.
Selects HTTPS Protocol.
Shows the current configuration.
Displays the last 20 commands entered during the current CLI session.
Sets HTTP request URL following IP address or hostname.
Sets the Username used to logon to HTTP server.
Stores the current configuration in permanent memory.

connection 2 (config-action-ftp_put-connection:	eth2 link state change:2) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port <number></number>	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.
write	Stores the current configuration in permanent memory.

connection 2 (config-action-http_post-connection:eth1 link state change:2) level commands	
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.

host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port <number></number>	Sets the Port number which HTTP server is listening to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.
write	Stores the current configuration in permanent memory.

connection 2 (config-action-ftp_put-connection:	eth1 link state change:2) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be connected to.
no host	Clears FTP server IP address or hostname.
no password	Sets default Password.
password <text></text>	Sets the Password used to logon to FTP server.
port <number></number>	Sets the Port number which FTP server is listening to.
protocol ftp	Selects FTP Protocol.
protocol ftps	Selects FTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the Username used to logon to FTP server.
write	Stores the current configuration in permanent memory.

connection 2 (config-action-http_post-connection:eth0 link state change:2) level commands	
clrscrn	Clears the screen.
default port	Sets default Port number.
default protocol	Sets default HTTP Protocol.
exit	Exits to the next higher level.

host <text></text>	Sets HTTP server IP address or hostname to be connected to.
no host	Clears HTTP server IP address or hostname.
no password	Clears the Password.
no url	Clears HTTP request URL.
no username	Clears the Username.
password <text></text>	Sets the Password used to logon to HTTP server.
port < <i>number</i> >	Sets the Port number which HTTP server is listenin to.
protocol http	Selects HTTP Protocol.
protocol https	Selects HTTPS Protocol.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
url <text></text>	Sets HTTP request URL following IP address or hostname.
username <text></text>	Sets the Username used to logon to HTTP server.
write	Stores the current configuration in permanent memory.
connection 2 (config-action-ftp_p	out-connection:eth0 link state change:2) level commands
clrscrn	Clears the screen.
default filename	Sets default FTP remote Filename.
default port	Sets default Port number.
default protocol	Sets default FTP Protocol.
default username	Sets default Username.
exit	Exits to the next higher level.
filename <text></text>	Sets FTP remote Filename.
host <text></text>	Sets FTP server IP address or hostname to be
IIUSI <iexi></iexi>	connected to.
	connected to. Clears FTP server IP address or hostname.
no host	
no host no password	Clears FTP server IP address or hostname.
no host no password password <text></text>	Clears FTP server IP address or hostname. Sets default Password.
no host no password password <text> port <number></number></text>	Clears FTP server IP address or hostname. Sets default Password. Sets the Password used to logon to FTP server. Sets the Port number which FTP server is listening
no host no password password <text> port <number> protocol ftp</number></text>	Clears FTP server IP address or hostname. Sets default Password. Sets the Password used to logon to FTP server. Sets the Port number which FTP server is listening to.
no host no password password <text> port <number> protocol ftp protocol ftps show</number></text>	Clears FTP server IP address or hostname. Sets default Password. Sets the Password used to logon to FTP server. Sets the Port number which FTP server is listening to. Selects FTP Protocol.
no host no password password <text> port <number> protocol ftp protocol ftps</number></text>	Clears FTP server IP address or hostname. Sets default Password. Sets the Password used to logon to FTP server. Sets the Port number which FTP server is listening to. Selects FTP Protocol. Selects FTPS Protocol.
no host no password password <text> port <number> protocol ftp protocol ftps show</number></text>	Clears FTP server IP address or hostname. Sets default Password. Sets the Password used to logon to FTP server. Sets the Port number which FTP server is listening to. Selects FTP Protocol. Selects FTPS Protocol. Shows the current configuration. Displays the last 20 commands entered during the

consoleflow (config-consoleflow) level commands	
active connection connection <number></number>	Sets active connection to Connection <number>.</number>
apply configuration updates always	Sets the action on configuration updates to Always, signifying that the device will always apply configuration updates.

memory.

Stores the current configuration in permanent

write

apply configuration updates if unchanged	Sets the action on configuration updates to If unchanged, signifying that the device will only apply configuration updates if no changes have been made locally.
apply configuration updates never	Sets the action on configuration updates to Never, signifying no configuration updates will be applied.
apply firmware updates disable	Restores the default action on new firmware (do not apply).
apply firmware updates enable	Automatically apply new firmware.
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default active connection	Restores the default active connection, which is Connection 1.
default apply configuration updates	Restores the default setting for configuration updates (Never).
default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
device description <text></text>	Sets the Device Description.
device id <text></text>	Sets the Device ID.
device key <text></text>	Sets the Device Key.
device name <text></text>	Sets the Device Name.
exit	Returns to the config level.
line <number></number>	Change to line configuration level.
no device description	Removes the Device Description.
no device id	Removes the Device ID.
no device key	Removes the Device Key.
no device name	Removes the Device Name.
reboot after firmware update disable	Could not find VarID 3600 in file /http/config/varid_help.mtxt
reboot after firmware update enable	Could not find VarID 3600 in file /http/config/varid_help.mtxt
reboot after update disable	Restores the default action when new configuration is applied (do not reboot) NOTE: The device will always reboot after a firmware update.
reboot after update enable	Enables automatic reboot when new configuration is applied.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the ConsoleFlow statistics.
state disable	Disables the ConsoleFlow client.
state enable	Enables the ConsoleFlow client.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.

credentials (ssl-credentials) level commands

clrscrn	Clears the screen.
create <credential name=""></credential>	Create a new credential name
delete <credential name=""></credential>	Delete existing credential by name
edit <credential name=""></credential>	View or edit an existing credential
exit	Exits to the ssl level.
show	Show existing credential names
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
device (device) level commands	
auto show tlog	Continuously displays the internal trouble log.
cirscrn	Clears the screen.
default long name	Restores the default product long name.
default short name	Restores the default product short name.
exit	Exit to the enable level.
long name <name></name>	Sets the product long name, displayed in command mode and the Web interface.
short name <name></name>	Sets the product short name, displayed in command mode and the Web interface. <name> = maximum of eight characters.</name>
show	Show system information
show hardware information	Displays information about the hardware.
show history	Displays the last 20 commands entered during the current CLI session.
show lines	Show line information
show memory	Displays current memory usage information.
show task state	Displays current task states.
show tlog	Displays the internal trouble log.
write	Stores the current configuration in permanent memory.
dhcpserver (config-dhcpd) level commands	
clrscrn	Clears the screen.
default end ip address	Restores end IP address of DHCP address pool to the default value.
default lease time	Restores the lease time to default value (24 hours).
default start ip address	Restores start IP address of DHCP address pool to the default value.
delete all static leases	Deletes all static leases.
delete static lease <instance></instance>	Deletes an entry from the static lease table <instance> = index of the entry being removed</instance>
end ip address <ip address=""></ip>	Sets the end IP address of DHCP address pool.
exit	Returns to the previous level.
lease time <hours></hours>	Sets the lease time. <number> = lease time in hours.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

start ip address <ip address=""></ip>	Sets the start IP address of DHCP address pool.
state disable	Disables DHCP server.
state enable	Enables DHCP server.
static leases < number>	Change to dhcpd static lease level.
write	Stores the current configuration in permanent memory.

diagnostics (config-diagnostics) level commands	
clrscrn	Clears the screen.
exit	Returns to the config level.
log	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:16) level c	ommands
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character < control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:15) level commands	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.

flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:14) level commands	
cirscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character

	has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:13) lev	rel commands
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character < control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:12) lev	rel commands
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.

flush stop character enable

Prevents the stop character from the Line from being forwarded to the network.

modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:11) lev	vel commands
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout < <i>milliseconds</i> >	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:10) level commar	nds
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:9) level command	ds
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
stop character < <i>control</i> >	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:8) level commands	
Clears the screen.	
Returns to the tunnel level.	
Does not flush serial data upon closing a tunneling connection.	
Flushes serial data buffer when a tunneling connection is closed.	
Forwards the stop character from the Line to the network.	
Prevents the stop character from the Line from being forwarded to the network.	
Does not watch the modem control pin to disconnect.	
Watches the modem control pin and disconnects if it is not asserted.	
Removes the stop character.	
Disables disconnect after timeout feature for tunneling sessions.	
Displays the current configuration.	
Displays the last 20 commands entered during the current CLI session.	
Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>	
Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>	
Stores the current configuration in permanent memory.	

disconnect (tunnel-disconnect:7) level commands	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.

flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:6) level commands	
cirscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:5) leve	el commands
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:4) leve	el commands
cirscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.

modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character < control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:3) level commands	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character < control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:2) level commands

clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

disconnect (tunnel-disconnect:1) level commands	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.

	Disable of the lead Of the section of the disable of
show history	Displays the last 20 commands entered during the current CLI session.
stop character <control></control>	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
timeout <milliseconds></milliseconds>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
discovery (config-discovery) level comma	ands
clear counters	Zeros Query Port counters
clrscrn	Clears the screen.
default upnp port	Resets the UPnP Server port to its default value (0x77FF).
exit	Returns to the config level.
no clear counters	Unzeros Query Port counters
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays statistics and information about the discovery services.
state disable	Disables the Query Port server.
state enable	Enables the Query Port server.
upnp port < <i>number</i> >	Sets the port number the UPnP server will use. <pre><number> = port number.</number></pre>
upnp state disable	Disables the UPnP server.
upnp state enable	Enables the UPnP server.
write	Stores the current configuration in permanent memory.
dns (dns) level commands	
clrscrn	Clears the screen.
exit	Exits to the enable level.
lookup <host_or_ip></host_or_ip>	Return a lookup on the DNS name or IP address.
show	Show DNS status.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
email (config-action-email:on scheduled i	reboot) level commands
alarm email email <number></number>	Specifies the email number to send when the alarm turns on.
alarm email none	Specifies no email when the alarm turns on.
alarm message <text></text>	Sets the email message to be sent when the alarm turns on.
alarm reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains on.

clrscrn	Clears the screen.
default alarm email	Specifies no email when the alarm turns on.
default normal email	Specifies no email when the alarm turns off.
exit	Exits to the next higher level.
no alarm message	Removes the alarm email message.
no alarm reminder interval	Only one message will be sent when the alarm turns on.
no normal message	Removes the normal email message.
no normal reminder interval	Only one message will be sent when the alarm turns off.
normal email email <number></number>	Specifies the email number to send when the alarm turns off.
normal email none	Specifies no email when the alarm turns off.
normal message <text></text>	Sets the email message to be sent when the alarm turns off.
normal reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains off.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

email (config-action-email:eth2 link state	change) level commands
alarm email email <number></number>	Specifies the email number to send when the alarm turns on.
alarm email none	Specifies no email when the alarm turns on.
alarm message <text></text>	Sets the email message to be sent when the alarm turns on.
alarm reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains on.
clrscrn	Clears the screen.
default alarm email	Specifies no email when the alarm turns on.
default normal email	Specifies no email when the alarm turns off.
exit	Exits to the next higher level.
no alarm message	Removes the alarm email message.
no alarm reminder interval	Only one message will be sent when the alarm turns on.
no normal message	Removes the normal email message.
no normal reminder interval	Only one message will be sent when the alarm turns off.
normal email email <number></number>	Specifies the email number to send when the alarm turns off.
normal email none	Specifies no email when the alarm turns off.
normal message <text></text>	Sets the email message to be sent when the alarm turns off.
normal reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains off.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
email (config-action-email:eth1 link state	change) level commands
alarm email email <number></number>	Specifies the email number to send when the alarm turns on.
alarm email none	Specifies no email when the alarm turns on.
alarm message <text></text>	Sets the email message to be sent when the alarm turns on.
alarm reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains on.
clrscrn	Clears the screen.
default alarm email	Specifies no email when the alarm turns on.
default normal email	Specifies no email when the alarm turns off.
exit	Exits to the next higher level.
no alarm message	Removes the alarm email message.
no alarm reminder interval	Only one message will be sent when the alarm turns on.
no normal message	Removes the normal email message.
no normal reminder interval	Only one message will be sent when the alarm turns off.
normal email <number></number>	Specifies the email number to send when the alarm turns off.
normal email none	Specifies no email when the alarm turns off.
normal message <text></text>	Sets the email message to be sent when the alarm turns off.
normal reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains off.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
email (config-action-email:eth0 link state	change) level commands
alarm email email < <i>number</i> >	Specifies the email number to send when the alarm turns on.
alarm email none	Specifies no email when the alarm turns on.
alarm message <text></text>	Sets the email message to be sent when the alarm turns on.
alarm reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains on.
clrscrn	Clears the screen.
default alarm email	Specifies no email when the alarm turns on.
default normal email	Specifies no email when the alarm turns off.
exit	Exits to the next higher level.
no alarm message	Removes the alarm email message.
no alarm reminder interval	Only one message will be sent when the alarm turns on.

no normal message	Removes the normal email message.
no normal reminder interval	Only one message will be sent when the alarm turns off.
normal email email <number></number>	Specifies the email number to send when the alarm turns off.
normal email none	Specifies no email when the alarm turns off.
normal message <text></text>	Sets the email message to be sent when the alarm turns off.
normal reminder interval <minutes></minutes>	Sets the time interval that messages will be sent while the alarm remains off.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

email 1 (email:1) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.

	· · · · · · · · · · · · · · · · · · ·
email 10 (email:10) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>

to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 11 (email:11) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email < <i>number</i> >	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.

auto show statistics	Continuously displays email statistics.
	Sets Cc addresses for email alerts. <text> = a</text>
cc <text></text>	quoted, semicolon separated list of email
clear log	addresses. Clears all entries from the mail log.
	_
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 13 (email:13) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.

clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email < <i>number</i> >	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 14 (email:14) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
	· ·

message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 15 (email:15) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.

no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.

Continuously displays email statistics.
Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
Clears all entries from the mail log.
Sets the email counters to zero.
Clears the screen.
Sets X-Priority for email alerts to 3 (normal).
Enters the configure email level.
Exits to the enable level.
Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
Removes the Cc addresses for email alerts.
Restores the email counters to the aggregate values.
Removes the file name, so the message body will be empty.
Removes the Reply To address for email alerts.
Removes subject used for email alerts.
Removes the To addresses for email alerts.
Sets X-Priority for email alerts to 2 (high).

priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.

Continuously displays email statistics.
Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
Clears all entries from the mail log.
Sets the email counters to zero.
Clears the screen.
Sets X-Priority for email alerts to 3 (normal).
Enters the configure email level.
Exits to the enable level.
Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
Removes the Cc addresses for email alerts.
Restores the email counters to the aggregate values.
Removes the file name, so the message body will be empty.
Removes the Reply To address for email alerts.
Removes subject used for email alerts.
Removes the To addresses for email alerts.
Sets X-Priority for email alerts to 2 (high).
Sets X-Priority for email alerts to 4 (low).
Sets X-Priority for email alerts to 3 (normal).
Sets X-Priority for email alerts to 1 (urgent).
Sets X-Priority for email alerts to 5 (very low).

Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
Sends an email using the current settings.
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
Displays the email log.
Displays email statistics.
Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
Stores the current configuration in permanent memory.

email 3 (email:3) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.

email 4 (email:4) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>

to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 5 (email:5) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 6 (email:6) level commands	

auto show statistics	Continuously displays email statistics.
	Sets Cc addresses for email alerts. <text> = a</text>
cc <text></text>	quoted, semicolon separated list of email
de su le s	addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 7 (email:7) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
t.	

clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email < <i>number</i> >	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 8 (email:8) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.

message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.
email 9 (email:9) level commands	
auto show statistics	Continuously displays email statistics.
cc <text></text>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default priority	Sets X-Priority for email alerts to 3 (normal).
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
message file <text></text>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.</text>
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.

no message file	Removes the file name, so the message body will be empty.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <text></text>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.</text>
send	Sends an email using the current settings.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.</text>
write	Stores the current configuration in permanent memory.

enable (enable) level commands	
auto show interfaces	Show interface statistics
auto show processes	Continuously show thread runtime information
clrscrn	Clears the screen.
configure	Enters the configuration level.
connect	Show name and number for lines.
connect line	Begin session on serial port.
device	Enters the device level.
disable	Exits the enable level.
dns	Enters the DNS level.
email <number></number>	Enters the configure email level.
exit	Exit from the system
filesystem	Enters the filesystem level.
iperf <params></params>	Run iperf with command line parameters passed in quoted string.
kill ssh <session></session>	Kills SSH session with index from "show sessions"
kill telnet <session></session>	Kills Telnet session with index from "show sessions"
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
ping <host></host>	Ping destination continuously with 5 second timeout
ping <host> <count></count></host>	Ping destination n times with 5 second timeout
ping <host> <count> <timeout></timeout></count></host>	Ping destination n times with x timeout (in seconds)
reload	Reboot system

reload factory defaults	Reload factory defaults to permanent storage
show	Show system information
show history	Displays the last 20 commands entered during the current CLI session.
show interfaces	Show interface statistics
show ip sockets	Show UDP/TCP state information
show lines	Show line information
show processes	Show thread runtime information
show sessions	Show active Telnet and SSH Sessions
ssh	Enters the SSH configuration level.
ssh <optclientusername> <host></host></optclientusername>	Begin SSH session on network <host>. The optClientUserName must match an SSH Client: Users configuration entry. Use "" in optClientUserName to prompt for host username and password.</host>
ssh <optclientusername> <host> <port></port></host></optclientusername>	Begin SSH session on network <host>:<port>. The optClientUserName must match an SSH Client: Users configuration entry. Use "" in optClientUserName to prompt for host username and password.</port></host>
ssl	Enters the SSL configuration level.
tcpdump <parameters></parameters>	dump traffic on a network
telnet <host></host>	Begin telnet session on network <host>.</host>
telnet <host> <port></port></host>	Begin telnet session on network <host>:<port>.</port></host>
trace route <host></host>	Trace route to destination
trace route <host> <protocol></protocol></host>	Trace route to destination using TCP, ICMP, or UDP
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xml	Enters the XML level.
eth1 link state change (config-action:eth1 link	state change) level commands
clrscrn	Clears the screen.
default delay	Resets alarm processing delay to its default value.
delay <seconds></seconds>	Sets the delay in processing the alarm. Alarm actions will not be executed if the cause is corrected within this time.
email	Enters the next lower level.
exit	Exits to the config alarm level.
ftp put	Enters the next lower level.
http post	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays statistics.
write	Stores the current configuration in permanent memory.

clrscrn

eth2 link state change (config-action:eth2 link state change) level commands

Clears the screen.

default delay	Resets alarm processing delay to its default value.
delay <seconds></seconds>	Sets the delay in processing the alarm. Alarm actions will not be executed if the cause is corrected within this time.
email	Enters the next lower level.
exit	Exits to the config alarm level.
ftp put	Enters the next lower level.
http post	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays statistics.
write	Stores the current configuration in permanent memory.
filesystem (filesystem) level commands	
cat <file></file>	Show the contents of a file
cd <directory></directory>	Change the current directory to the specified directory
clrscrn	Clears the screen.
cp <source file=""/> <destination file=""></destination>	Copy an existing file
dump <file></file>	Show contents of a file as a hex dump
exit	Exits to the enable level.
format	Format the file system and lose all data
Is	Show all files and directories in the current directory
Is <directory></directory>	Show all files and directories in the specified directory
mkdir <directory></directory>	Create a directory
mv <source file=""/> <destination file=""></destination>	Move a file on the file system
pwd	Print working directory
rm <file></file>	Remove a file
rmdir <directory></directory>	Remove a directory
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show file system statistics
show tree	Show all files and directories from current directory
tftp get <source file=""/> <destination file=""> <host></host></destination>	Get a file using TFTP
tftp get <source file=""/> <destination file=""> <host> <port></port></host></destination>	Get a file using TFTP
tftp put <source file=""/> <destination file=""> <host></host></destination>	Put a file using TFTP
tftp put <source file=""/> <destination file=""> <host> <port></port></host></destination>	Put a file using TFTP
touch <file></file>	Create a file
ftp (config-ftp) level commands	
clrscrn	Clears the screen.
	Datuma to the confinitional
exit	Returns to the config level.
exit show	Returns to the config level. Displays the current configuration.

show statistics	Displays the FTP statistics.
state disable	Disables the FTP server.
state enable	Enables the FTP server.
write	Stores the current configuration in permanent memory.

ftp put (config-action-ftp_put:on sched	duled reboot) level commands
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the FTP Put reminder interval. FTP Put is sent once only.
reminder interval <minutes></minutes>	Sets the FTP Put reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

ftp put (config-action-ftp_put:eth2 link state change) level commands	
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the FTP Put reminder interval. FTP Put is sent once only.
reminder interval <minutes></minutes>	Sets the FTP Put reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

ftp put (config-action-ftp_put:eth1 link state change) level commands	
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.

mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the FTP Put reminder interval. FTP Put is sent once only.
reminder interval <minutes></minutes>	Sets the FTP Put reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
ftp put (config-action-ftp_put:eth0 link state cha	nge) level commands
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the FTP Put reminder interval. FTP Put is sent once only.
reminder interval <minutes></minutes>	Sets the FTP Put reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
gateway (config-gateway) level commands	
add forwarding rule <start port=""> <end port=""> <protocol> <ip></ip></protocol></end></start>	Add a forwarding rule without a name.
add forwarding rule <start port=""> <end port=""> <target port=""> <pre> <pre> port> <pre> <ip> port> <pre> <ip> content</ip></pre></ip></pre></pre></pre></target></end></start>	Add a forwarding rule based on ip address without a name.
add forwarding rule with name <name> <start port=""> <end port=""> <pre> <pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></end></start></name>	Add a forwarding rule with a name.
add forwarding rule with name <name> <start port=""> <target port=""> <end port=""> <pre> <ip> <ip> </ip></ip></pre></end></target></start></name>	Add a forwarding rule based on ip address with a name.
add route <network> <gateway> <interface> <metric></metric></interface></gateway></network>	Add a static route without a name.
add route with name <name> <network> <gateway> <interface> <metric></metric></interface></gateway></network></name>	Add a static route with a name.
clrscrn	Clears the screen.
default operating mode	Restores operating mode to the default value (Disabled).
default router ip address	Restores IP address of router to the default value.
default wan interface	Restores preferred WAN interface to the default

value.

delete all routes	Deletes all static routes.
delete all rules	Deletes all port forwarding rules.
delete route <instance></instance>	Deletes an entry from the static routes <instance> = index of the entry being removed.</instance>
delete rule <instance></instance>	Deletes an entry from the port forwarding rules <pre><instance> = index of the entry being removed.</instance></pre>
dhcpserver	Enters the dhcpserver level.
exit	Returns to the config level.
firewall disable	Disables firewall on WAN interface.
firewall enable	Enables firewall on WAN interface.
no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
operating mode disabled	Disables routing on WAN interface.
operating mode gateway	Enables routing with NAT on WAN interface.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
primary dns <ip address=""></ip>	Sets the IP address of the primary DNS server.
router ip address <ip address="" cidr=""></ip>	Sets the IP address of router. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
secondary dns <ip address=""></ip>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show routing table	Show current routing table.
show status	Show gateway configuration and status.
static route < number>	Change to config gateway static route level.
wan interface <text></text>	Sets the preferred WAN interface. <text> = interface name.</text>
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:16:1) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key < <i>hexadecimal</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

	0.4.4
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode
•	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
	· · · · · · · · · · · · · · · · · · ·

protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

•
mmands
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.

credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:14:1) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the
	SSL client.
default protocol	Restores the default protocol as "TCP".

default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	ıe.i.yi
host 1 (tunnel-connect-host:13:1) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:12:1) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
	,

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:11:1) level comman	<mark>ds</mark>
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <i><binary></binary></i>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:10:1) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocortop	Uses TCP protocol with AES encryption for connect
protocol tcp aes	mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:9:1) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:8:1) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes Des TCP protocol with AES encryption for connect mode tunneling.		
secure protocols ssl3 disable secure protocols tls1.0 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocol tls1.2 disable secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show Shows the current configuration. Show statistics show connection statistics show statistics show connection statistics show statistics show connection statistics show connections with other devices. <text> =</text>	protocol tcp aes	
secure protocols ssl3 enable Enables the protocol. secure protocols tls1.0 disable secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.2 disable Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. Sets the connecting. Solve servication of the server certificate when connecting. Solve servication of the server certificate when connecting. Solve servication of the server certificate when connecting. Solve the current configuration in permanent memory. Solve the current configuration in permanent memory. Solve the current configuration in permanent memory. Solve the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent h</number></number></number></number></number></milliseconds></milliseconds></text>	protocol telnet	
secure protocols tls1.0 disable Secure protocols tls1.1 onable Secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.1 enable Secure protocols tls1.2 disable Secure protocols tls1.2 disable Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive itimeout. <milliseconds> = timer value, in milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the value in milliseconds. Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the current tonel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *123ABC *123ABC* *12</number></number></number></milliseconds></milliseconds></text>	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 enable secure protocols tls1.2 disable protocol secure protocols tls1.2 enable protocol udp protocol udp protocol udp aes show Show show the current configuration. Disables the protocol Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> tcp keep alive interval <milliseconds> tcp keep alive probes <number> stop user timeout <milliseconds> ctp user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the number of TCP retransmissions. williseconds> = timeout value, in milliseconds. Sets the number of TCP retransmissions. williseconds> = timeout value, in milliseconds. Sets the number of TCP retransmissions. williseconds> = timeout value, in milliseconds. Sets the remout for TCP retransmissions. williseconds> = timeout value, in milliseconds. Sets the connecting. Requires verification of the server certificate when connecting. Stops verification of the server certificate when connecting. Stores the current configuration in permanent memory. Institute of the server certificate when connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A BC 12.3a bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></number></number></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Uses UDP protocol or connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> number of TCP keep alive probes. <number> number of TCP keep alive probes. <number> number of TCP keep</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable protocol udp protocol udp protocol udp protocol udp show show show istory show statistics show connection statistics show lumining connections with other devices. ctext> = SSH user name for use when establishing tunneling connections with other devices. ctext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <number> = number of TCP retransmi</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show W Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. ctext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> top user timeout <milliseconds> sets the timeout for TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP teransmissions. sets the timeout for TCP teransmissions. self set enable Sets the timeout for TCP teransmissions. self set enable to the server certificate when connecting. Sets the current configuration in permanent memory. Inst 1 (tunnel-connect-host-7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC 712 3A BC 12.3A, BC 12.3A, BC 12.3A, BC 12.3A, BC 12.3A, BC 12.3A, BC with up to 14 bytes. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte if it contains spaces.</text></number></number></milliseconds></number></number></milliseconds></milliseconds>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol stls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show structures tonfiguration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> step user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retarnsisions. stilliseconds> = timeout value, in milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. step user timeout <milliseconds> Sets the timeout for TCP retarnsisions. smilliseconds> = timeout value, in milliseconds> Sets the timeout for TCP retarnsisions. smilliseconds> = timeout value, in milliseconds> Sets the timeout for TCP retarnsisions. smilliseconds> = timeout value, in milliseconds Skips verification of the server certificate when connecting. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. Inst 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12:3a.bc Note that quotes must enclose the v</text></milliseconds></number></milliseconds></number></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes protocol udp aes show Show be current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show statistics show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> stop user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. stop user timeout <milliseconds> stop user timeout or top ternamissions. connecting. Skips verification of the server certificate when connecting. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. nost 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A, BC 12.3a, bc 12:3a, bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
protocol udp aes show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. solution of TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Sets the immout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the current configuration in permanent memory. Inost 1 (tunnel-connect-host:7:1) level commands Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*123ABC*12ABC*</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
protocol udp aes show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the current configuration in permanent memory. Inost 1 (tunnel-connect-host:7:1) level commands Sets the current configuration in permanent memory. Inost 1 (tunnel-connect-host:7:1) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together by the separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC" 12</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Inost 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value if it contains that quotes must enclose the value</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	protocol udp aes	Uses UDP protocol with AES encryption for connect
show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time <milliseconds></milliseconds></text>	show history	
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 1 (tunnel-connect-host7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable validate certificate enable Sets the current configuration in permanent memory. Tost 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections with up to 10 contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections with up to 10 contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections with u</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> sets the timeout for TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Nost 1 (tunnel-connect-host:7:1) level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 20 decrypt key with up to 30 decrypt key total to 21 decrypt key with up to 30 decrypt key total to 22 decrypt key with up to 30 decrypt key total to 23 decrypt key with up to 30 decrypt key total total total and sets the timeout of TCP keep alive probes. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <mi>milliseconds. Sets the timeout of TCP keep alive probes. Sets the connect tunnel AES decrypt key with up to 30 decrypt key total total timeout of TCP keep alive probes. Sets the connect tunnel AES decrypt key with up to 30 decrypt key total total timeout of TCP keep alive probes. Sets the connect tunnel AES decrypt key with up to 30 decrypt key total total timeout of TCP keep alive probes. Sets the connect tunnel AES decrypt key with up to 30 decrypt key total total timeout of TCP keep alive probes. Sets the connect tunnel AES decrypt key with up to 30 decrypt key total total timeou</mi></text></milliseconds></milliseconds></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. host 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to Sets the connect tunnel AES decrypt key with up to</text>	tcp user timeout <milliseconds></milliseconds>	
connecting. Stores the current configuration in permanent memory. host 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 connections. Sets the connect tunnel AES decrypt key with up to 50 connections.</text>	validate certificate disable	·
memory. host 1 (tunnel-connect-host:7:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	·
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 1 (tunnel-connect-host:7:1) level com	mands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	aes decrypt key text < text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.

secure protocols ist3.0 disable secure protocols ist3.1 disable secure protocols ist3.1 disable secure protocols ist3.1 disable secure protocols ist3.1 disable secure protocols ist3.2 disable secure protocol ist4.2 disable secure protocol ist5.2 disable secure protocol. Secure disable di		
secure protocols tis1.0 enable secure protocols tis1.1 disable secure protocols tis1.1 disable secure protocols tis1.2 disable secure protocols tis1.2 disable secure protocols tis1.2 enable secure protocols tis1.2 enable secure protocols tis1.2 enable Enables the protocol. secure protocols tis1.2 enable Enables the protocol. Secure protocols tis1.2 enable Enables the protocol. Secure protocol dy Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show support the secure to end tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds. <milliseconds="timer" <number="" alive="" and="" connect="" enables="" for="" in="" keep="" milliseconds.="" mode="" probes="" sets="" tcp="" the="" timer.="" tunneling="" value,=""> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <number="number" =="" alive="" alive<="" keep="" number="" of="" probes.="" tcp="" td=""><td>secure protocols ssl3 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds.></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Jesseure protocol udp aes show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <ext> = SSH user name. Sets the TCP keep alive idle time. This is the initial top keep alive idle time. Amilliseconds> show and set the time timeout. Amilliseconds> immediately and sets the timeout. Amilliseconds = timer value, in milliseconds. Top keep alive probes <number> step keep alive probes <number> step keep alive probes <number> = number of TCP keep alive probes. <number> = numbe</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></ext>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show statistics Show statistics Show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time <milliseconds> tcp keep alive interval <milliseconds> cp user timeout <milliseconds> cp user timeout <milliseconds> step the enable certificate disable validate certificate enable write Sets the TCP keep alive for connect mode tunneling and sets the timer. smilliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <number="" alive="" certificate="" connecting.="" cornect="" keep="" of="" probes.="" server="" sets="" tcp="" td="" the="" tunne<="" when=""><td>secure protocols tls1.0 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable Enables the protocol. Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show show statistics show connections statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> <mi>ctp keep alive probes </mi></milliseconds> <milliseconds. <milliseconds="" alive="" and="" connect="" enables="" for="" keep="" mode="" sets="" tcp="" the="" timer.="" tunneling=""> = timer value, in milliseconds> <mi>ctp user timeout <milliseconds> <milliseconds. (tunnel-connect-hostset)="" <="" alive="" and="" certificate="" commands="" configuration="" connecting.="" current="" disable="" dress="" enable="" for="" in="" instit="" keep="" level="" lext="" memory.="" number="" of="" permanent="" probes.="" retransmissions.="" server="" sets="" skips="" stores="" tcp="" the="" timeout="" validate="" verification="" when=""> Sets the remote host to establish tunneling connections with. <lext> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123AEC *12 3A BC* *1</lext></milliseconds.></milliseconds></mi></milliseconds.></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.2 enable protocol udp protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show Show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds = timeout value, in timeout value, in milliseconds = timeout value, in timeout value, in timeout value,</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp protocol udp aes Show Show sterver tonfiguration. Show sterver tonfiguration. Show statistics Show connection statistics Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text>= SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds = timer value, in milliseconds. Sets the number of TCP keep alive probes. connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds = timer value, in milliseconds. Sets the number of TCP keep alive probes. connect mode tunneling and sets the timer. Thilliseconds Sets the number of TCP keep alive probes. connect mode tunneling and sets the timer. Trilliseconds Sets the funder of TCP keep alive probes. connect mode tunneling and sets the timer. Trilliseconds> Sets the funder of TCP keep alive probes. connect-number of TCP keep alive probes. Sets the timeout for TCP keep alive probes. connect-number of TCP keep alive probes. Sets the timeout for TCP keep alive probes. Requires verification of the server certificate when connecting. Set</milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
protocol udp protocol udp aes Show Show sterver tonfiguration. Show sterver tonfiguration. Show statistics Show connection statistics Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text>= SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds = timer value, in milliseconds. Sets the number of TCP keep alive probes. connect mode tunneling and sets the timer. Thilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. Thilliseconds = timer value, in milliseconds. Sets the number of TCP keep alive probes. connect mode tunneling and sets the timer. Thilliseconds Sets the number of TCP keep alive probes. connect mode tunneling and sets the timer. Trilliseconds Sets the funder of TCP keep alive probes. connect mode tunneling and sets the timer. Trilliseconds> Sets the funder of TCP keep alive probes. connect-number of TCP keep alive probes. Sets the timeout for TCP keep alive probes. connect-number of TCP keep alive probes. Sets the timeout for TCP keep alive probes. Requires verification of the server certificate when connecting. Set</milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
protocol udp aes show Show be current configuration. Displays the last 20 commands entered during the current CLI session. Show she current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> step user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the number of TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. stores the current configuration in permanent memory. Inst 1 (tunnel-connect-hostical) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by the digit it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by the adjacent hex digits. Bytes may run together or be separated by two adjacent</text></text></milliseconds></milliseconds></number></number></number></number></milliseconds></number></milliseconds></milliseconds></milliseconds></text>	·	·
show history show history show statistics show statistics show connection statistics show connection statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. validate certificate disable Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. It (tunnel-sonnect-hosts) level commands Sets the remote host to establish tunneling connections with. <lext> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12.3a,bc 12.3a;bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated of two digits. Bytes may run together or be separated by two adjacent hex digits. Byte</lext></number></number></number></milliseconds></milliseconds></text>	protocol udp aes	
show history Show statistics Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <numbers **stillseconds="" =="" alive="" keep="" number="" of="" probes.="" retransmission.="" sets="" tcp="" the=""> = timeout for TCP retransmission. **stillseconds> = timeout value, in milliseconds. **Stillseconds> = timeout value, in mi</numbers></milliseconds></milliseconds></milliseconds></text>	show	-
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time <milliseconds> to milliseconds> to milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds. (tunnel-connect-hosts)="" 1="" <le="" <milliseconds="timeout" <multiple="" alive="" and="" certificate="" commands="" conders="number" configuration="" connect="" connecting.="" connections="" current="" disable="" enables="" establish="" for="" host="" in="" keep="" level="" lost="" memory.="" milliseconds.="" mode="" number="" of="" permanent="" probes.="" remote="" requires="" retransmissions.="" server="" sets="" skips="" stores="" tcp="" the="" timer.="" to="" tunneling="" validate="" value,="" verification="" when="" with.="">dext = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by set and provides must enclose the value if it contains spaces.</milliseconds.></milliseconds></text>	show history	Displays the last 20 commands entered during the
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate disable Sets the current configuration in permanent memory. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Rost 1 (tunnel-connect-host:6:1) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by 2 separated by 3 single character. Note that quotes must enclose the value if it contains spaces.</text></text></milliseconds></number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Post 1 (tunnel-connect-host:6:1) level commands** **Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC 12.3A BC 12.3a.bc 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by sets and punctuation: 123ABC 12.3 abc 12.3</text></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Tost 1 (tunnel-connect-host:6:1) level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated</text></milliseconds></number></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. bost 1 (tunnel-connect-host:6:1) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated</text></text>	tcp keep alive probes < number>	
validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Nost 1 (tunnel-connect-host:6:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. **Nost 1 (tunnel-connect-host:6:1) level commands address < text> Sets the remote host to establish tunneling connections with. < text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated	validate certificate disable	
memory. Nost 1 (tunnel-connect-host:6:1) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	write	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	host 1 (tunnel-connect-host:6:1) level commands	
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>		Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>	aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:5:1) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 1 (tunnel-connect-host:4:1) level command	s
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:3:1) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 1 (tunnel-connect-host:2:1) level commar	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent
hoot 4 (confin hoot) () lovel commands	memory.
host 1 (config-host:1) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:16:10) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:15:10) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	incinory.
host 10 (tunnel-connect-host:14:10) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:13:10) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

	Enghles TCD keep alive for compact was do town alive
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:12:10) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value

address <text></text>	connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	•
host 10 (tunnel-connect-host:11:10) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:10:10) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:9:10) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:8:10) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:7:10) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols tls1.0 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable Disables the protocol. Secure protocols tls1.2 disable protocol udp Disables the protocol. Enables the protocol. Secure protocols tls1.2 disable protocol udp Disables the protocol. Secure protocols tls1.2 enable protocol udp Disables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocol with AES encryption for connect mode tunneling. Show the current configuration. Show show connection with AES encryption for connect mode tunneling. Show the current configuration. Show show connection statistics show connection statistics show connection statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. **milliseconds* = timer value, in milliseconds* = timer value, in milliseconds. Sets the TCP keep alive for connect mode tunneling and sets the timer. **milliseconds* = timer value, in milliseconds. Top user timeout <**milliseconds* = timer value, in milliseconds* = timer use, in milliseconds = timer use, in milliseconds. Sets the number of TCP keep alive probes. **cumber* = number of TCP keep alive probes. **cumber* = number of TCP keep alive probes. **sets the mumber of TCP keep alive probes. **sets the mumber of TCP retransmissions. **validate certificate disable **validate certificate disable **validate certificate on the server certificate when connecting. **validate certificate enable **validate certificate on the server certificate when connecting. **validate certi</text>		E 11 (1 (1)
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocol udp Uses UDP protocol for connect mode tunneling. protocol udp protocol udp Uses UDP protocol with AES encryption for connect mode tunneling. Show show shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show statistics show connection statistics sets the SSH user name for use when establishing uneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive immeout. <milliseconds. <milliseconds="" alive="" and="" connect="" enables="" for="" keep="" mode="" sets="" tcp="" the="" timer.="" tunneling=""> = timer value, in milliseconds. tcp keep alive probes <number> step user timeout <milliseconds> cumber> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <numbers <numbers="number" =="" alive="" keep="" number="" of="" pr<="" probes.="" tcp="" td=""><td>secure protocols ssl3 enable</td><td>Enables the protocol.</td></numbers></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds.></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocol tls1.2 enable secure protocol tls1.2 enable protocol udp Uses UDP protocol or connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Shows the current configuration. Shows the current configuration. Shows the current configuration. Show statistics show connection statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> cp user timeout <milliseconds> = timeout for TCP keep alive probes. Sets the timer. This is the initial keep alive interval <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds> = timeout value, in milliseconds = timeo</milliseconds></milliseconds></number></milliseconds></milliseconds></text>	·	·
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics show connection statistics show connections with other devices, <text> = SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> stop user timeout <milliseconds> sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <number="number" <number<="" =="" alive="" keep="" number="" of="" probes.="" tcp="" td=""><td>·</td><td>·</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></number></milliseconds></milliseconds></milliseconds></text></text>	·	·
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol up protocol up protocol up protocol up protocol up up ses UDP protocol for connect mode tunneling. Juses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds. <milliseconds.="timer" <number="" alive="" and="" connect="" enables="" for="" in="" keep="" milliseconds.="" mode="" probes="" sets="" tcp="" the="" timer.="" tunneling="" value,=""> tcp user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sulidate certificate disable solidate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 123A,BC 123A,BC 123A,BC 125ABC byte sire presented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two dijectors and the stables is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note th</text></number></number></milliseconds></milliseconds.></text>	·	·
secure protocols tis1.2 enable protocol udp protocol udp protocol udp aes Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics	secure protocols tls1.1 enable	Enables the protocol.
protocol udp protocol udp aes Show Show statistics Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connectors with or milliseconds and set the time. This is the initial top keep alive interval miltiseconds Sets the TCP keep alive idle time. This is the initial top keep alive probes number> Enables TCP keep alive for connect mode tunneling and sets the time. This is the initial top keep alive interval miltiseconds Enables TCP keep alive for connect mode tunneling and sets the timer. This is the initial seep alive interval miltiseconds Enables TCP keep alive for connect mode tunneling and sets the timer. This is the initial seep alive probes number Enables TCP keep alive for connect mode tunneling and sets the timer. This is the initial seep alive probes number Enables TCP keep alive for connect mode tunneling and sets the timer. This is the initial seep alive timeout. This is the initial seep alive timeout. This is the initial seep alive timeout. This is the initial top keep alive interval nitiliseconds Sets the number of TCP keep alive probes. number To P keep alive probes number Sets the mumber of TCP keep alive probes. number To P keep alive probes. number To P keep alive probes number To P keep alive probes. number Sets	secure protocols tls1.2 disable	Disables the protocol.
protocol udp aes show show show bistory show history show statistics show shatistics show statistics show shatistics show current CLI session. Show state as SH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds> = timer value, in milliseconds. top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> step user timeout <milliseconds> sets the number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the number of TCP keep alive probes. Sets the number of TCP keep alive probes. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Institute the server certificate when connections with. <1ext> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC '123ABC' 12,3ABC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by the separated by the separated by two adjacent hex digits. Bytes may run together or be separated by the separated by two adjacent the digits. Bytes may run together or be separated by the separated by the sepa</milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text></text>	secure protocols tls1.2 enable	Enables the protocol.
show Shows the current configuration. Show shistory Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. top keep alive probes <number></number></milliseconds></milliseconds></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> top keep alive probes <number> top keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP teap alive probes. <number <nu<="" <number="number" =="" alive="" number="" of="" probes.="" tcp="" td="" teap=""><td>protocol udp aes</td><td>Uses UDP protocol with AES encryption for connect mode tunneling.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <stent <milliseconds="" timeout=""> = timeout value, in milliseconds. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. Tost 10 (tunnel-connect-host:6:10) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12 3A BC</text></milliseconds></stent></number></number></number></number></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set user name. Set sthe TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = time out value, in milliseconds> = time value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds = timeout value, in milliseconds = timeout value, in milliseconds = timeout value, in milliseconds. Sets the timeout value, in milliseconds. Sets the timeout value, in milliseconds = timeout value, in millisecond</milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></milliseconds></text>	show history	
ssh username <text> SSH user name. SSH user name. SSH user name. SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. step user timeout <milliseconds> step user timeout to TCP retransmissions. <nilliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Fost 10 (tunnel-connect-host:6:10) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 10.23a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes ma</text></nilliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> tcp keep alive probes <number> tcp keep alive probes <number> tcp user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <<="" <number="" probes.="" td=""><td>ssh username <text></text></td><td>tunneling connections with other devices. <text> = SSH user name.</text></td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> commeters = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Tost 10 (tunnel-connect-host:6:10) level commands** address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated</text></text></milliseconds></number></number></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
number> = number of TCP keep alive probes. **tcp user timeout <milliseconds> **sets the timeout for TCP retransmissions. **validate certificate disable **sets the timeout for TCP retransmissions. **sets the timeout value, in milliseconds. Skips verification of the server certificate when connecting. **requires verification of the server certificate when connecting. **sets the current configuration in permanent memory. **sets the remote host to establish tunneling connections with. <=text> = IP address or host name of the remote host. **Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. **Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. **Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by the set that quotes must enclose the value if it contains spaces. **Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. host 10 (tunnel-connect-host:6:10) level commands address < text> Sets the remote host to establish tunneling connections with. < text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by desire presented by two adjacent hex digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated	tcp keep alive probes < number>	
validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Nost 10 (tunnel-connect-host:6:10) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. Inost 10 (tunnel-connect-host:6:10) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by the contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	validate certificate disable	
memory. Nost 10 (tunnel-connect-host:6:10) level commands	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	write	,
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	host 10 (tunnel-connect-host:6:10) level comm	nands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>		Sets the remote host to establish tunneling connections with. <text> = IP address or host name</text>
aes decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>	aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
by optional punctuation: 123ABC "12 3A BC"	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:5:10) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	1 -
host 10 (tunnel-connect-host:4:10) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

nds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:2:10) level com	ımands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
initial send set <text></text>	or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ands
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 10 (config-host:10) level commands	,
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:16:11) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:15:11) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 11 (tunnel-connect-host:14:11) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:13:11) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:12:11) level commands	

	· · · · · ·
host 11 (tunnel-connect-host:12:11) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:11:11) level comm	ands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:10:11) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
•	Sets the remote port to use for connect mode
port <number></number>	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:9:11) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:8:11) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in
	binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	connection. Within [] use binary decimal up to 255
initial send set <text> no address</text>	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections.</text>
no address no aes decrypt key	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key.</text>
no address no aes decrypt key no aes encrypt key	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key.</text>
no address no aes decrypt key no aes encrypt key no credentials	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection.</text>
no address no aes decrypt key no aes encrypt key	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string.</text>
no address no aes decrypt key no aes encrypt key no credentials no initial send no port	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.</text>
no address no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.</text>
no address no aes decrypt key no aes encrypt key no credentials no initial send no port	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default.</text>
no address no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number></text>
no address no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username no tcp user timeout	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling.</number></text>
no address no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username no tcp user timeout port <number></number>	connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number></text>

protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:7:11) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	abarastar Nata that quates recet englace the colors
	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:6:11) level commar	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:5:11) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

, ,	
host 11 (tunnel-connect-host:4:11) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
·	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,e.,,
host 11 (tunnel-connect-host:3:11) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:2:11) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre></pre> <p< td=""></p<>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	· · · · · ·
host 11 (tunnel-connect-host:1:11) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <i><binary></binary></i>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent
	memory.
host 11 (config-host:11) level command	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:16:12) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 12 (tunnel-connect-host:15:12) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 12 (tunnel-connect-host:14:12) lev	rel commands
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 12 (tunnel-connect-host:13:12) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:12:12) level (commands
	Sets the remote host to establish tunneling

h and 40 (turn all agrees at h and 40.40) law	
host 12 (tunnel-connect-host:12:12) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	·
host 12 (tunnel-connect-host:11:12) leve	l commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:10:12) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
•	Sets the remote port to use for connect mode
port <number></number>	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 12 (tunnel-connect-host:9:12) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:8:12) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

12 en	
	optional punctuation: 123ABC "12 3A BC" 2,3A,BC 12.3a.bc 12:3a:bc Note that quotes must aclose the value if it contains spaces.
aes decrypt key text < text> 16 ch if it	ets the connect tunnel AES decrypt key with up to bytes. Each byte is represented by a single taracter. Note that quotes must enclose the value t contains spaces.
aes encrypt key <hexadecimal> he by 12</hexadecimal>	ets the connect tunnel AES encrypt key with up to bytes. Each byte is represented by two adjacent ex digits. Bytes may run together or be separated optional punctuation: 123ABC "12 3A BC" 2,3A,BC 12.3a.bc 12:3a:bc Note that quotes must aclose the value if it contains spaces.
aes encrypt key text <text> 16</text>	ets the connect tunnel AES encrypt key with up to bytes. Each byte is represented by a single paracter. Note that quotes must enclose the value t contains spaces.
auto show statistics show	ow connection statistics
clrscrn Cle	ears the screen.
	elects the RSA/DSA certificates by name for the SL client.
default protocol	estores the default protocol as "TCP".
default secure protocols	estores the default secure protocol selections.
default tcp keep alive idle time De	efaults the TCP keep alive idle time.
detailit ten keen alive interval	estores the default 45 second connect mode TCP ep alive timeout.
default tcp keep alive probes De	efaults the TCP keep alive probes.
exit Ex	kits to the next higher level.
initial send binary <i><binary></binary></i> bin co	ets the host connect tunnel Initial Send text owing for binary characters. binary format that will be sent out the network upon binnection. Within [] use binary decimal up to 255 hex up to 0xFF.
initial send set <text> = a</text>	ets the host connect tunnel Initial Send text. <text>ascii string that will be sent out the network upon onnection.</text>
no address	emoves the remote host address used to establish nneling connections.
Do ooo doomint koy	emoves the connect tunnel AES decrypt key.
	emoves the connect tunnel AES encrypt key.
no aes encrypt key	* * * * * * * * * * * * * * * * * * * *
no aes encrypt key no credentials Re	ears the RSA/DSA certificate selection.
no aes encrypt key no credentials cle no initial send Re	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string.
no aes encrypt key no credentials cle no initial send Re no port Re	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string. emoves the remote port used to establish tunnel ennections.
no aes encrypt key no credentials Cle no initial send Re no port co no ssh username Re	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string. emoves the remote port used to establish tunnel ennections. emoves the SSH user name.
no aes encrypt key no credentials Cle no initial send Re no port co no ssh username Re	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string. emoves the remote port used to establish tunnel ennections.
no aes encrypt key no credentials Cle no initial send Re no port no port no ssh username no tcp user timeout Re Se	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string. emoves the remote port used to establish tunnel innections. emoves the SSH user name.
no aes encrypt key no credentials Cle no initial send Re no port Re no ssh username no tcp user timeout port <number> set tur protocol ssh Re Re</number>	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string. emoves the remote port used to establish tunnel ennections. emoves the SSH user name. estores the default. ets the remote port to use for connect mode enneling. <number> = number of the port to use. ses SSH protocol for connect mode tunneling.</number>
no aes encrypt key no credentials Cle no initial send Re no port Re no port Re no tcp user timeout Re port <number> Se tur protocol ssh Us</number>	ears the RSA/DSA certificate selection. emoves the host connect tunnel Initial Send string. emoves the remote port used to establish tunnel innections. emoves the SSH user name. estores the default. ets the remote port to use for connect mode inneling. <number> = number of the port to use.</number>

protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Secure protocols sts1.0 disable Secure protocols tts1.0 disable Secure protocols tts1.1 disable Secure protocols tts1.1 disable Secure protocols tts1.1 disable Secure protocols tts1.1 disable Secure protocols tts1.2 disable Secure protocol tts1.2 disable Secure protocol tts1.2 disable Secure protocol usp Uses UDP protocol of connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = \$\$SH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> tcp keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> Sets the timeout for TCP keep alive probes. = timer value, in milliseconds> Sets the timeout for TCP keep alive probes. Validate certificate disable Sets the immeut of the server certificate when connecting. Sets the current configuration in permanent memory. Nost 12 (tunnel-connect-host:7:12) level commands Sets the rome host to establish tunneling connections with. <te> = the address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Sytes may run together or be separated by optional punctuation: 123ABC *123ABC* *123ABC* *123ABC* *123ABC* *123ABC* *123ABC* *123ABC</te></milliseconds></milliseconds></milliseconds></text>		
secure protocols ssl3 disable secure protocols ssl3 enable Secure protocols ssl3.0 enable Secure protocols tls1.0 enable Secure protocols tls1.1 enable Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol sls1.2 enable Disables the protocol. Enables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol sls1.2 enable Disables the protocol. Secure protocol. Secure protocol sls1.2 enable Disables the protocol. Secure protocol. Secure protocol sls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol sls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol. Secure protocol sls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol sls1.2 enable	protocol tcp aes	
secure protocols sts10 enable secure protocols tst1.0 disable secure protocols tst1.0 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.2 disable Secure protocols tst1.2 enable Secure protocol udp Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number certificate="" of="" server="" td="" the="" w<=""><td>protocol telnet</td><td>. , ,</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	protocol telnet	. , ,
secure protocols sts10 enable secure protocols tst1.0 disable secure protocols tst1.0 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.2 disable Secure protocols tst1.2 enable Secure protocol udp Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number certificate="" of="" server="" td="" the="" w<=""><td>secure protocols ssl3 disable</td><td></td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols ssl3 disable	
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp protocol udp protocol udp aes show Show show show show show istory show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> step keep alive probes <number> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step keep alive probes. step user timeout split yellow in the server certificate when connecting. Sets the timeout for TCP retransmissions. split seconds = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. Institute texts = lP address or host name of the remote host. Sets the remote host to establish tunneling connections with . texts = lP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC*12 3A BC*12 3A BC*12 3A BC*14 3A BC*</milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></milliseconds></number></number></milliseconds></text>	secure protocols ssl3 enable	
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocol tldp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds <number="" =="" alive="" in="" keep="" milliseconds.="" probes="" tcp="" timer="" value,=""> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> number of TCP keep alive probes. <numbe< td=""><td>secure protocols tls1.0 disable</td><td>·</td></numbe<></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 disable	·
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show bistory Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. ctext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. emilliseconds> trop keep alive interval <milliseconds> tcp keep alive interval <milliseconds> tcp keep alive probes <number> ctp user timeout <milliseconds> tcp user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP retransmissions. <milliseconds> = timer value, in milliseconds> sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> tcp user timeout <milliseconds> Sets the timeout of TCP retransmissions. <milliseconds> = timeout value, in milliseconds> Sets the connecting. Sets the current configuration in permanent memory. Activate the server certificate when connecting. Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123AB C" 123ABC 12:3a bc 12:3a bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is feroresented by two adjacent hex digits. Bytes may run together</text></text></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></number></milliseconds></milliseconds>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. text- Sets the TCP keep alive idle time. This is the initial keep alive interval mailtiseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds Ests the timeout of TCP keep alive probes. Sets the timeout of TCP keep alive probes. Sets the timeout for TCP retransmissions. All time time time time time time time time	secure protocols tls1.1 disable	Disables the protocol.
secure protocol sts1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. stop user timeout <milliseconds> sets the milliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. nost 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text></number></number></number></milliseconds></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
secure protocol sts1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. stop user timeout <milliseconds> sets the milliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. nost 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text></number></number></number></milliseconds></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the connecting. Sets the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 t</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration.	·	·
Show statistics show statistics show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP retransmissions. <number> = number of the server certificate when connecting. Sets the timeout for TCP retransmissions. <number> = number of the server certificate when connecting. Stops verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands aeddress <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 to 12 to</text></text></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></text>		Uses UDP protocol with AES encryption for connect
show history Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Most 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces.</text></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds></text>	show	-
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set she TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the
tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idne time of the initial keep alive idne time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. top keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable validate certificate enable validate certificate enable stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></number></number></milliseconds></milliseconds></text>	show statistics	show connection statistics
keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123ABC" 123ABC 123a.bc 123a.bc 123a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds></milliseconds></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate enable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 sets the connect tunnel AES decryp</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 sets the connect t</text>	validate certificate disable	
memory. host 12 (tunnel-connect-host:7:12) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> 5 sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> 5 decrypt key text < text> 5 decrypt key with up to 2 decrypt key text < text> 5 decrypt key with up to 2 decrypt key text < text> 5 decrypt key with up to 2 decrypt key with up to 3 decrypt key text < text> 5 decrypt key with up to 3 decrypt key with up to 3 decrypt key text < text> 6 decrypt key with up to 3 decrypt key with up to 3 decrypt key text < text> 6 decrypt key text < text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key text> 6 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key text> 6 decrypt key w</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 12 (tunnel-connect-host:7:12) level co	mmands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <i><hexadecimal></hexadecimal></i>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	aes decrypt key text <text></text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:6:12) level commar	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 12 (tunnel-connect-host:5:12) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	momory.
host 12 (tunnel-connect-host:4:12) leve	l commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 12 (tunnel-connect-host:3:12) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 12 (tunnel-connect-host:2:12) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
initial send set <text></text>	or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ands
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent
host 12 (config-host:12) level command	memory.
cirscrn	Clears the screen.
default protocol default remote port	Restores the default value of the protocol (Telnet). Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:16:13) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 13 (tunnel-connect-host:15:13) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	inemory.
host 13 (tunnel-connect-host:14:13) level comm	ands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	•
host 13 (tunnel-connect-host:13:13) level comm	nands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

host 13 (tunnel-connect-host:12:13) level commands	
write	Stores the current configuration in permanent memory.
validate certificate enable	Requires verification of the server certificate when connecting.
validate certificate disable	Skips verification of the server certificate when connecting.
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>

	, ,
host 13 (tunnel-connect-host:12:13) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
	or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 13 (tunnel-connect-host:11:13) level com	mands
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:10:13) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 13 (tunnel-connect-host:9:13) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:8:13) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

	Uses TCP protocol with AES encryption for connect
protocol tcp aes	mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:7:13) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:6:13) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent have digite. Bytes may run tegether or be congreted.

hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	
secure protocols tls1.1 enable	Disables the protocol. Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 13 (tunnel-connect-host:5:13) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 13 (tunnel-connect-host:4:13) leve	l commands
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

nds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 13 (tunnel-connect-host:2:13) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
initial send set <text></text>	or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 13 (tunnel-connect-host:1:13) level comma	ands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when
write	connecting. Stores the current configuration in permanent
	memory.
host 13 (config-host:13) level command	S
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:16:14) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:15:14) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 14 (tunnel-connect-host:14:14) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	•
host 14 (tunnel-connect-host:13:14) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:12:14) level commands	

	,
host 14 (tunnel-connect-host:12:14) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	annuation Military and the second of the second
	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:11:14) level comm	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <i><binary></binary></i>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:10:14) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
•	Sets the remote port to use for connect mode
port <number></number>	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:9:14) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:8:14) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes Uses TCP protocol with AES encryption for connect mode tunneling.		
secure protocols ssl3 disable secure protocols tls1.0 disable secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.2 disable Secure protocols tls1.2 disable Secure protocols tls1.2 disable Disables the protocol. Secure protocols tls1.2 disable Secure protocol udp Disables the protocol. Enables the protocol. Enables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show sthe current configuration. Show show the current configuration. Show statistics Show sconnection statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for the protocol with explaint of the server devices. <text> = SSH user name for the protocol with explaint of the server devices. <text> = SSH user name for use when establishing tunneling connections. <text> = SSH user name for the protocol with explaint of the server devices. <text> = SSH user name for the protocol with explaint of the server certificate when connecting. Sets the timeout for TCP keep alive probes. Sets the timeout for TCP keep alive probes. Sets the timeout for TCP retransmissions. **Anilliseconds*** = timeout value, in milliseconds. **Stipper support of the server certificate w</text></text></text></text></text></text></text></text></text></text>	protocol tcp aes	
secure protocols sts10 enable secure protocols tis1.0 enable secure protocols tis1.0 enable secure protocols tis1.1 enable secure protocols tis1.1 enable secure protocols tis1.1 enable secure protocols tis1.2 enable Disables the protocol. Enables the protocol. Enables the protocol. Secure protocols tis1.2 enable Disables the protocol. Enables the protocol. Secure protocols tis1.2 enable Disables the protocol. Enables the protocol. Enables the protocol. Secure protocols tis1.2 enable Disables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TOP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TOP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> tcp keep alive probes <number> tcp user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number of="" se<="" td="" the=""><td>protocol telnet</td><td>· · · · · · · · · · · · · · · · · · ·</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></milliseconds></text>	protocol telnet	· · · · · · · · · · · · · · · · · · ·
secure protocols tis1.0 disable secure protocols tis1.1 disable secure protocols tis1.2 disable Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> sets the connect in the timer. TCP keep alive probes. sets the number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the timeout for TCP retarnamissions. sets the timeout for TCP retarnamissions. sets the current configuration in permanent memory. store the current configuration in permanent for the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123ABC" 123ABC" 123ABC "12</milliseconds></milliseconds></text></text>	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Disables the protocol. secure protocols tls1.2 enable protocol udp protocol udp aes show Show store the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step user timeout of TCP keep alive probes. <milliseconds> = timeout value, in milliseconds. Sets the number of TCP keep alive probes. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Tost 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC" 12 3A BC total stap to the ser</text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 enable Secure protocol tlp Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> sets the number of TCP keep alive probes. <number> <number> <number <numbers="number" alive="" keep="" of="" probes.="" tcp="" tcp<="" td=""><td>secure protocols tls1.0 disable</td><td>Disables the protocol.</td></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show be current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. dext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> connections connections connecting. Sets the mumber of TCP keep alive probes. sets the timer. TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the timer. <milliseconds< a=""> = timer value, in milliseconds. Sets the timeout for TCP retransmissions. sets the timer of TCP keep alive probes. sets the timeout for TCP retransmissions. sets the timeout for TCP retransmissions. sets the timeout value, in milliseconds. Sets the timeout value, in milliseconds. Sets the connecting. Solve or the current configuration in permanent memory. Tost 14 (tunnel-connect-host-7-14) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC '123 AB C' 12.3A BC 12.3a bc 12.3a bc Note that quotes must enoble the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex di</milliseconds<></milliseconds></milliseconds></milliseconds>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp protocol udp protocol udp aes Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. text-> Sets the SSH user name for use when establishing tunneling connections with other devices. text-> Sets the TCP keep alive idle time. This is the initial keep alive interval mailtiseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds top keep alive probes number> Sets the number of TCP keep alive probes. Sets the number of TCP keep alive probes. **Chumber> = number of TCP keep alive probes. **Chumber> = number of TCP keep alive probes. **Sets the timeout for TCP retransmissions. **milliseconds> = timeout value, in milliseconds. **Skips verification of the server certificate when connecting. **Skips verification of the server certificate when connecting. **Stores the current configuration in permanent memory. **Total Cunnel-connect-host:7:14) level commands **Sets the remote host to establish tunneling connections with. <a **sets="" 12="" 12.3a,="" aes="" an<="" and="" bc="" connect="" contains="" decrypt="" enclose="" href="mailto: Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC " if="" it="" key="" must="" note="" quotes="" spaces.="" td="" that="" the="" to="" tunnel="" up="" value="" with=""><td>secure protocols tls1.1 disable</td><td>Disables the protocol.</td>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol stls1.2 enable protocol udp protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. *milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> step user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP tetransissions. <number> = number of TCP retransissions. <number> = number of TCP retransissions. <number> = number of TCP retransissions. <number> = number of TCP retransisons. <number <number="number" =="" number="" o<="" of="" retransisons.="" tcp="" td=""><td>secure protocols tls1.1 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes protocol udp aes show Show be current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show statistics show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the mount of TCP keep alive probes. Sets the mount for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the mount for TCP retransmissions. <numbers =="" illiseconds="" number="" of="" retransmissions.="" set="" tcp=""> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. set the number of TCP retransmissions. set the onnecting. Skips verification of the server certificate when connecting. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. nost 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12 3A, BC 12 3A, BC 12 3A, BC to 2 3A BC* 12 3A, BC to 2 4 5 4 4 5 4 4 5 4 4 4 4 4 4 4 4 4 4 4</text></numbers></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
show Show she current configuration. Shows the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. validate certificate disable validate certificate disable validate certificate enable Sets the runner configuration in permanent memory. iost 14 (tunnel-connect-host:7:14) level commands Sets the runner host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces.</text></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
show Show she current configuration. Shows the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Requires verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Validate certificate enable Sets the current configuration in permanent memory. Iost 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 15 bytes. Each byte is represented by contains spaces. Sets the connect tunnel AES decrypt key with up to 15 bytes. Each byte is the connect tunnel AES decry</text></milliseconds></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	protocol udp	·
show history show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. cumber> = number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the timeout for TCP retransmissions. set the current configuration of the server certificate when connecting. Requires verification of the server certificate when connecting. stores the current configuration in permanent memory. stores the current configuration in permanent memory. stores the current configuration in permanent memory. stores the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces.</number></milliseconds></milliseconds></text></text>	protocol udp aes	
show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number></number></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set she TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write</milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive itimeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable validate certificate enable validate certificate enable stop user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Tost 14 (tunnel-connect-host:7:14) level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 24 contains spaces.</text></milliseconds></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Nost 14 (tunnel-connect-host:7:14) level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 19,000 and punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces.</text></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. validate certificate disable validate certificate enable Stores the current configuration in permanent memory. nost 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2as decrypt key text state. Sets the connect tunnel AES decrypt key with up to 2as decrypt key text state. Sets the connect tunnel AES decrypt key with up to 2as decrypt key text state. Sets the connect tunnel AES decrypt key with up to 2as decrypt key text state.</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate disable validate certificate enable write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 s</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. host 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.</text>	validate certificate disable	
memory. host 14 (tunnel-connect-host:7:14) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2 certain the connect tunnel AES decrypt key with up to 2 certain the connect tunnel AES decrypt key with up to 2 certain the connect tunnel AES decrypt key with up to 3 certain the connec</text>	validate certificate enable	· ·
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 14 (tunnel-connect-host:7:14) level con	mmands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	aes decrypt key text <text></text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.

secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:6:14) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	Sets the connect tunnel AES encrypt key with up to
aes encrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.

secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:5:14) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.

protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.	hoot 14 (tunnal connect hoot; 4:44) level	commando
connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.</text>	nost 14 (tunnel-connect-nost:4:14) level	commands
aes decrypt key <hexadecimal> aes decrypt key <hexadecimal> by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.</hexadecimal></hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
aes decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. suuto show statistics</text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics show connection statistics	aes decrypt key text < text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
aes encrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.</text>	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	aes encrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
clrscrn Clears the screen.	auto show statistics	show connection statistics
	cirscrn	Clears the screen.

credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:3:14) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols default tcp keep alive idle time	Restores the default secure protocol selections.
dotault ton koon alive idle times	Defaults the TCP keep alive idle time.

default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:2:14) level commar	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 14 (tunnel-connect-host:1:14) level com	ımands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection Within Duce himery desired on to OFF
	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 14 (config-host:14) level command	ls .
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:16:15) lev	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.

secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:15:15) level comm	ands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode
<u> </u>	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.

protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:14:15) leve	I commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.

credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show statistics	show connection statistics
onow stationes	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:13:15) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.

default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	•
host 15 (tunnel-connect-host:12:15) level comm	nands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:11:15) leve	l commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	-
host 15 (tunnel-connect-host:10:15) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

Removes the remote host address used to establish tunneling connections.
Removes the connect tunnel AES decrypt key.
Removes the connect tunnel AES encrypt key.
Clears the RSA/DSA certificate selection.
Removes the host connect tunnel Initial Send string.
Removes the remote port used to establish tunnel connections.
Removes the SSH user name.
Restores the default.
Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
Uses SSH protocol for connect mode tunneling.
Uses SSL protocol for connect mode tunneling.
Uses TCP protocol for connect mode tunneling.
Uses TCP protocol with AES encryption for connect mode tunneling.
Uses Telnet protocol (with IAC) for connect mode tunneling.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Uses UDP protocol for connect mode tunneling.
Uses UDP protocol with AES encryption for connect mode tunneling.
Shows the current configuration.
Displays the last 20 commands entered during the current CLI session.
show connection statistics
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
Skips verification of the server certificate when

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:9:15) leve	l commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
	Removes the remote host address used to establish
no address	tunneling connections.
no address no aes decrypt key no aes encrypt key	tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode
	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:8:15) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:7:15) level com	ımands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value f it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent nex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value f it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
detailit ton keen alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit E	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no addroce	Removes the remote host address used to establish cunneling connections.
	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes encrypt key no credentials	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection.
no aes encrypt key no credentials no initial send	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string.
no aes encrypt key no credentials no initial send F no port F	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
no aes encrypt key no credentials cono initial send no port no ssh username F	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.
no aes encrypt key no credentials cono initial send no port no ssh username Gradentials Fraction in the state of the stat	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
no aes encrypt key no credentials no initial send F no port no ssh username no tcp user timeout F Port crumbos	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.
no aes encrypt key no credentials Cono initial send For the series of th	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode cunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling.</number>
no aes encrypt key no credentials cono initial send no port no ssh username no tcp user timeout port <number> protocol ssh protocol ssl</number>	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode cunneling. <number> = number of the port to use.</number>

protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Secure protocols sts1.0 disable Secure protocols tts1.0 disable Secure protocols tts1.1 disable Disables the protocol. Secure protocols tts1.1 disable Disables the protocol. Secure protocols tts1.1 disable Disables the protocol. Secure protocols tts1.1 disable Secure protocols tts1.2 disable Secure protocols tts1.2 disable Disables the protocol. Secure protocols tts1.2 disable Disables the protocol. Secure protocols tts1.2 disable Disables the protocol. Secure protocol sts1.2 disable Disables the protocol. Secure protocol sts1.2 disable Disables the protocol. Secure protocol sts1.2 enable Enables the protocol. Secure protocol ust protocol dist1.2 disable Disables the protocol. Secure protocol sts1.2 disable Disables the protocol. Secure protocol. Secure protocol sts1.2 disable Disables the protocol. Secure protocol sts1.2 disable Disables the protocol. Secure protocol. Secure protocol sts1.2 disable Disables the protocol. Secure protocol sts1.2 disable Disables the protocol. Show to secure protocol sts1.2 disable disable disable Disables the protocol. Secure protocol sts1.2 disable disable Disables the protocol. Disables the protocol. Disables the protocol for sometiment disable d		
secure protocols ssl3 disable secure protocols ssl3 enable Secure protocols ssl3.0 enable Secure protocols tls1.0 enable Secure protocols tls1.1 enable Secure protocols tls1.2 disable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol tls1.2 enable Disables the protocol. Enables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol tls1.2 enable Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol. Secure protocol tls1.2 enable Secure protocol tls1.2 enable Secure protocol tls1.2 enable Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Secure protocol test tempotocol tunnel Acs decreption enable Disables the protocol. Secure protocol tis1.2 enable Secure protocol tis1.2 enable Secure protocol tis1.2 enable Secure protocol tis1.2 ena	protocol tcp aes	
secure protocols sts10 enable secure protocols tst1.0 disable secure protocols tst1.0 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.2 disable Secure protocols tst1.2 enable Secure protocol udp Uses UDP protocol for connect mode tunneling, Drotocol udp Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	protocol telnet	· · · · · · · · · · · · · · · · · · · ·
secure protocols sts10 enable secure protocols tst1.0 disable secure protocols tst1.0 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.2 disable Secure protocols tst1.2 enable Secure protocol udp Uses UDP protocol for connect mode tunneling, Drotocol udp Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp protocol udp protocol udp aes show Show show show show show istory show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step timeout split user of TCP keep alive probes. <mi>milliseconds> = timeout value, in milliseconds. step user timeout <milliseconds> step timeout value, in milliseconds. steps verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Tost 15 (tunnel-connect-host 6:15) level commands Sets the remote host to establish tunneling connections with . text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC" 12 3A BC total size by set to tall if it contains spaces. Sets the connect tunnel AES decrypt key with up to 15 bytes. Each byte if it contains spaces.</milliseconds></mi></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></text>	secure protocols ssl3 enable	
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Secure protocols tls1.2 enable protocol udp Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show by the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds <number="" =="" alive="" in="" keep="" milliseconds.="" probes="" tcp="" timer="" value,=""> sets the number of TCP keep alive probes. <number> <number <numbers="number" alive="" keep="" of="" probes.="" tcp="" tcp<="" td=""><td>secure protocols tls1.0 disable</td><td>·</td></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 disable	·
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval. <mi>whilliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <mi>whilliseconds = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> <sets <number="" alive="" keep="" number="" of="" probes.="" tcp="" the=""> = number of TCP keep alive probes. <number> = number of TCP retransmissions. Sets the timeout for TCP retransmissions. Sets the connecting. Sets the current configuration in permanent memory. Some the current configuration in permanent memory. Some the current configuration in permanent memory. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123 AB C" 12.3 AB C 12.3</number></number></number></number></number></number></number></number></number></number></number></sets></number></number></mi></mi></text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> top keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. smilliseconds> = timeout value, in milliseconds validate certificate disable styp verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12 3A, BC 12 3A, BC 12 3A, BC 12 3A, BC tables and tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12 3A, BC 12 3A, BC 12 3A, BC* 13 3A, BC 12 3A, BC* 14 2 3A, BC* 15 3A, BC* 16 3C 4C 4C</text></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol sts1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. squildate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. Institute the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 set the value if it contains spaces.</number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
secure protocol sts1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. squildate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. Institute the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 set the value if it contains spaces.</number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the connecting. Sets the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 t</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the immount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the connecting. Sets the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 t</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	·	·
show history Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Most 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 102:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>		Uses UDP protocol with AES encryption for connect
show history Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Most 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 102:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel AES decrypt key with up to 10 connections tunnel</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set she TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the
tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write</milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show statistics	show connection statistics
keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></number></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds></milliseconds></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 sets the connect t</text>	validate certificate disable	
memory. host 15 (tunnel-connect-host:6:15) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> 5 sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> 5 decrypt key text < text> 5 decrypt key with up to 2 decrypt key text < text> 5 decrypt key with up to 2 decrypt key text < text> 5 decrypt key with up to 2 decrypt key with up to 3 decrypt key text < text> 5 decrypt key with up to 3 decrypt key with up to 3 decrypt key text < text> 6 decrypt key with up to 3 decrypt key text < text> 6 decrypt key text < text> 6 decrypt key text < text> 6 decrypt key with up to 3 decrypt key text < text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key text> 6 decrypt key with up to 3 decrypt key text> 6 decrypt key text> 6 decrypt key text> 6 decrypt key text> 6</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 15 (tunnel-connect-host:6:15) level co	mmands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	aes decrypt key text <text></text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
	-
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:5:15) level comn	nands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

enclose the value if it contains space Sets the connect tunnel AES encry 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. auto show statistics show connection statistics Clears the screen.	pt key with up to by a single
aes encrypt key text <text> 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. auto show statistics clrscrn 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. Show connection statistics Clears the screen.</text>	by a single
clrscrn Clears the screen.	
credentials <text> Selects the RSA/DSA certificates by SSL client.</text>	y name for the
default protocol Restores the default protocol as "To	CP".
default secure protocols Restores the default secure protocol	ol selections.
default tcp keep alive idle time Defaults the TCP keep alive idle time	ne.
default tcp keep alive interval Restores the default 45 second corkeep alive timeout.	nect mode TCP
default tcp keep alive probes Defaults the TCP keep alive probes	3.
exit Exits to the next higher level.	
Sets the host connect tunnel Initial allowing for binary characters. binary format that will be sent out the connection. Within [] use binary decorr hex up to 0xFF.	ary> = string in ne network upon
Sets the host connect tunnel Initial initial send set <text> = ascii string that will be sent out th connection.</text>	
no address Removes the remote host address tunneling connections.	used to establish
no aes decrypt key Removes the connect tunnel AES of	decrypt key.
no aes encrypt key Removes the connect tunnel AES e	encrypt key.
no credentials Clears the RSA/DSA certificate sele	ection.
no initial send Removes the host connect tunnel li	nitial Send string.
no port Removes the remote port used to e connections.	stablish tunnel
no ssh username Removes the SSH user name.	
no tcp user timeout Restores the default.	
port <number> Sets the remote port to use for contunneling. <number> = number of the</number></number>	
protocol ssh Uses SSH protocol for connect mod	de tunneling.
protocol ssl Uses SSL protocol for connect mod	
protocol tcp Uses TCP protocol for connect mod	
protocol tcp aes Uses TCP protocol with AES encry mode tunneling.	•
protocol telnet Uses Telnet protocol (with IAC) for tunneling.	connect mode
secure protocols ssl3 disable Disables the protocol.	
secure protocols ssl3 enable Enables the protocol.	
secure protocols tls1.0 disable Disables the protocol.	
secure protocols tls1.0 enable Enables the protocol.	
secure protocols tls1.1 disable Disables the protocol.	
secure protocols tls1.1 enable Enables the protocol.	

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:4:15) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 15 (tunnel-connect-host:3:15) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:2:15) level comma	ınds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:1:15) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre></pre> <p< td=""></p<>

	Sets the timeout for TCP retransmissions.
tcp user timeout <milliseconds></milliseconds>	<milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 15 (config-host:15) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:16:16) leve	l commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
	Disables the protocol.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 disable secure protocols ssl3 enable	Enables the protocol.

secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:15:16) level comma	ands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

auto show statistics auto show statistics show connection statistics clears the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol default secure protocols default secure protocols default top keep alive interval default top keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary connection. Within [] use binary deciral untel methods on one store the not open according to the next of the send to the next on one connection. Removes the remote port used to sets the protocol selections. 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol as "TCP". Restores the default secure protocol selections. Defaults the TCP keep alive protocos. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. chinarys = string in binary format that will be sent out the network upon connection. Within [] use binary deciral up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send texttext> = socii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. no aed decrypt key Removes the connect tunnel AES decrypt key. no credentials Clears the RSA/DSA certificate selection. Removes the host connect tunnel hitial Send string. Removes the host connect tunnel hitial Send string. Removes the host connect mode tunneling. Default type of the port to use for connect mode tunneling. Less StH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses SSL protocol (with IAC) for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling		0
Clears the screen. Credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default secure protocol selections. default top keep alive interval Restores the default secure protocol selections. default top keep alive interval Restores the default 45 second connect mode TCP keep alive imeout. Restores the default 45 second connect mode TCP keep alive imeout. Sets the host connect tunnel Initial Send text allowing for binary characters. solinary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. solinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascil string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Sets the remote port to use for connect mode tunneling. Less SSL protocol for connect mode tunneling. Sets the remote port to use for connect mode tunneling. Less SSL protocol for connect mode tunneling. Less SSL protocol for connect mode tunneling. Less TCP protocol for connect m</text></text>	aes encrypt key text <text></text>	character. Note that quotes must enclose the value
Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default top keep alive idle time Defaults the TCP keep alive idle time. default top keep alive idle time Restores the default 45 second connect mode TCP keep alive idle time. Restores the default 45 second connect mode TCP keep alive timeout. default top keep alive probes Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. https://doi.org/10.100/j.ner/ Sets the host connect tunnel Initial Send text allowing for binary characters. https://doi.org/ Sets the host connect tunnel Initial Send text allowing for binary decimal up to 255 or hex up to 0xFT. Sets the host connect tunnel Initial Send text. https://doi.org/ Sets the host connect tunnel Initial Send text. https://doi.org/ Sets the host connect tunnel Initial Send text. https://doi.org/ Removes the remote host address used to establish tunneling connections. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port to use for connect mode tunneling. https://doi.org/ Removes the remote port to use for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protoco	auto show statistics	show connection statistics
default protocol default protocol default protocol default secure protocols default secure protocols default secure protocols default secure protocols default top keep alive idle time default top keep alive idle time default top keep alive interval default top keep alive interval default top keep alive probes exit Sets to the next higher level. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. shinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no aes decrypt key no aes encrypt key no aes encrypt key no credentials no initial send Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the nemote port used to establish tunnel no port Removes the sen tunnel AES encrypt key. Clears the RSH user name. Removes the default. Sets the host connect tunnel finitial Send string. Removes the default. Sets the host connect tunnel nitial Send string. Removes the bost connect tunnel finitial Send string. Removes the protocol for connect mode tunneling. rummber> set the remote port to use for connect mode tunneling. rummber> protocol ssh Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol tcp uses TCP protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol tenes Protocol ssl disable Disables the protocol. Enables the protocol.</text>	clrscrn	Clears the screen.
default secure protocols default top keep alive idle time default top keep alive idle time default top keep alive interval default top keep alive interval default top keep alive interval default top keep alive probes exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary charactersbinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text allowing for binary charactersbinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send texttext> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunnelingclumber> protocol ssh Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol	credentials <text></text>	•
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive interval default tcp keep alive probes exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters chinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text allowing for binary characters chinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text text> = ascil string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no ase decrypt key no ase encrypt key no ase encrypt key no ase sencrypt key no ase the connect tunnel AES encrypt key. no eredentials Clears the RSA/DSA certificate selection. Removes the host connect tunnel AES encrypt key. no port Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling(number> = number of the port to use. Uses SSL protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol tcp Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for conn	default protocol	Restores the default protocol as "TCP".
default tcp keep alive interval default tcp keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. shinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text allowing for binary characters. shinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text= <br="" address="" aes="" ascil="" be="" certificate="" clears="" connect="" connection.="" connections.="" decrypt="" default.="" dsa="" encrypt="" establish="" for="" host="" initial="" key.="" mode="" network="" no="" out="" port="" remote="" removes="" restores="" rsa="" selection.="" send="" sent="" sets="" string="" that="" the="" to="" tunnel="" tunneling="" tunneling.="" upon="" use="" used="" will=""></text=> Sets the remote port to use for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol tcp aes Protocol tcp Uses TCP protocol (with IAC) for connect mode tunneling. Disables the protocol. Secure protocols tis1.0 disable Secure protocols tis1.0 disable Disables the protocol. Enables the protocol. Secure protocols tis1.1 enable Enables the protocol. Disables the protocol.	default secure protocols	Restores the default secure protocol selections.
default tcp keep alive interval	default tcp keep alive idle time	Defaults the TCP keep alive idle time.
Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text Sets the host connect tunnel Initial Send text. Sets the host connect tunnel Initial Send text. Sets the host connect tunnel Initial Send text. Sets the host connect tunnel Initial Send text. Sets the host connect tunnel Initial Send text. Sets the host connect tunnel Initial Send text. Sets the host connect tunnel Initial Send text. Sets the remote host address used to establish tunneling connections. no aeddress no aes decrypt key Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Initial Send string. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol stall AES encryption for connect mode tunneling. Uses TCP protocol stall AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for	default tcp keep alive interval	
Sets the host connect tunnel Initial Send text allowing for binary characters, sbinary> = string in binary characters, sbinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. no address Removes the remote host address used to establish tunneling connections. no aes decrypt key Removes the connect tunnel AES decrypt key. no aes encrypt key Removes the connect tunnel AES encrypt key. no credentials Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. no set user timeout Removes the SSH user name. no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh Uses SSH protocol for connect mode tunneling. protocol ssl Uses SSL protocol for connect mode tunneling. protocol tcp Uses TCP protocol for connect mode tunneling. protocol tcp aes Uses TCP protocol for connect mode tunneling. protocol tenet Uses TCP protocol (with IAC) for connect mode tunneling. secure protocols stl3.0 disable Disables the protocol. secure protocols ttl1.0 disable Disables the protocol. secure protocols ttl1.1 disable Disables the protocol. secure protocols ttl1.1 disable Enables the protocol.</number></text>	default tcp keep alive probes	Defaults the TCP keep alive probes.
allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. no address no aed decrypt key no aes encrypt key no aes encrypt key no credentials no initial send Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used for connect mode tunneling. Sets the remote port to use for connect mode tunneling. International port no sh username Removes the SSH user name. no top user timeout Restores the default. port <number> Sets the remote port to use for connect mode tunneling. Tunneling. <number> = number of the port to use. Uses SSL protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for c</number></number></text>	exit	Exits to the next higher level.
initial send set <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the nest connect tunnel Initial Send string. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSL protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Disables the protocol. Secure protocols tls1.0 disable Secure protocols tls1.0 disable Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 enable Secure protocols tls1.2 disable Disables the protocol.</number></number></text>	initial send binary binary>	allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255</binary>
tunneling connections. no aes decrypt key no aes encrypt key no aes encrypt key no credentials Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. no set username Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol seh Protocol sel Protocol tcp Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp aes Protocol telnet Uses TCP protocol (with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Disables the protocol. Secure protocols tls1.0 disable Secure protocols tls1.0 enable Enables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 enable Enables the protocol. Secure protocols tls1.1 enable Secure protocols tls1.2 disable Disables the protocol.</number>	initial send set <text></text>	= ascii string that will be sent out the network upon
no aes encrypt key no credentials Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. no ssh username Removes the SSH user name. Removes the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols sl3 enable Enables the protocol. Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol. Disables the protocol. Enables the protocol. Disables the protocol.</number>	no address	
no credentials no initial send Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Sets the remote port to use for connect mode tunneling. no top user timeout Restores the default. Sets the remote port to use for connect mode tunneling. number Protocol ssh Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol top Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Disables the protocol. Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no initial send Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Enables the protocol. Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Enables the protocol. Secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Disables the protocol.</number></number>		· · ·
Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Protocol ssl Protocol tcp Protocol tcp Protocol tcp aes Protocol telnet Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tsl1.0 disable Secure protocols tsl1.1 disable Secure protocols tsl1.1 enable Secure protocols tsl1.2 disable Secure protocols tsl1.2 disable Secure protocols tsl1.2 disable Disables the protocol. Disables the protocol. Enables the protocol. Disables the protocol. Disables the protocol. Enables the protocol. Disables the protocol.</number>	no credentials	Clears the RSA/DSA certificate selection.
connections. no ssh username no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. protocol ssl protocol tcp protocol tcp protocol tcp protocol tcp aes Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. secure protocols ssl3 disable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Enables the protocol. Secure protocols tls1.1 enable Enables the protocol. Disables the protocol.</number></number>	no initial send	Removes the host connect tunnel Initial Send string.
no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. protocol ssl protocol tcp protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Disables the protocol. Secure protocols tls1.0 disable Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol. Disables the protocol. Secure protocols tls1.1 enable Enables the protocol. Disables the protocol. Disables the protocol. Disables the protocol.</number></number>	no port	
port <number> port <number> port <number> Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Uses Telnet protocol. Secure protocols ssl3 disable Disables the protocol. Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 enable Secure protocols tls1.2 disable Disables the protocol. Enables the protocol.</number></number></number></number>	no ssh username	Removes the SSH user name.
tunneling. <number> = number of the port to use. protocol ssh protocol ssl protocol tcp protocol tcp uses TCP protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Disables the protocol. Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Enables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 enable Enables the protocol. Disables the protocol. Disables the protocol. Disables the protocol.</number>	no tcp user timeout	Restores the default.
protocol ssh protocol ssl protocol ssl protocol tcp protocol tcp aes protocol telnet secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable protocol ssh Uses SSL protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol.	nort < number>	
protocol ssl protocol tcp Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Enables the protocol. Enables the protocol.	•	
protocol tcp protocol tcp aes Disables the protocol. Becure protocols tls1.0 enable Becure protocols tls1.1 disable Becure protocols tls1.1 enable Brotocol tcp aes Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Disables the protocol. Enables the protocol. Disables the protocol. Enables the protocol. Disables the protocol. Disables the protocol.	•	
protocol tcp aes Disables the protocol. Becure protocols tls1.0 enable Becure protocols tls1.1 enable Becure protocols tls1.2 disable Disables the protocol. Disables the protocol. Enables the protocol. Disables the protocol. Enables the protocol. Disables the protocol. Disables the protocol.	·	·
protocol telnet protocol telnet protocol telnet protocol telnet secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Enables the protocol. Disables the protocol. Disables the protocol. Disables the protocol.	protocol tcp	
tunneling. secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Enables the protocol. Disables the protocol. Disables the protocol.	protocol tcp aes	mode tunneling.
secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Secure protocols tls1.2 disable Disables the protocol.	protocol telnet	tunneling.
secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Enables the protocol. Disables the protocol.	secure protocols ssl3 disable	·
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Disables the protocol.	secure protocols ssl3 enable	·
secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable Disables the protocol. Disables the protocol.	secure protocols tls1.0 disable	·
secure protocols tls1.1 enable Enables the protocol. secure protocols tls1.2 disable Disables the protocol.	secure protocols tls1.0 enable	·
secure protocols tls1.2 disable Disables the protocol.	secure protocols tls1.1 disable	·
·	secure protocols tls1.1 enable	·
secure protocols tls1.2 enable Enables the protocol.	secure protocols tls1.2 disable	·
	secure protocols tls1.2 enable	Enables the protocol.

protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	•
host 16 (tunnel-connect-host:14:16) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.

	Calasta the DCA/DCA cortificates by name for the
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

snow statistics	snow connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:13:16) level o	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.

show connection statistics

show statistics

	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,e.,,
host 16 (tunnel-connect-host:12:16) leve	el commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:11:16) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>

most to (turnici-connect-nost. 11.10) icv	or communus
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
	or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
	Uses TCP protocol with AES encryption for connect
protocol tcp aes	mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must</text>
connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must</text>
16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255
or hex up to 0xFF.

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:1-9:16) lev	vel commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 16 (tunnel-connect-host:8:16) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:7:16) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value f it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent nex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value f it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
detailit ton keen alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit E	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no addroce	Removes the remote host address used to establish cunneling connections.
	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes encrypt key no credentials	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection.
no aes encrypt key no credentials no initial send	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string.
no aes encrypt key no credentials no initial send F no port F	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
no aes encrypt key no credentials cono initial send no port no ssh username F	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.
no aes encrypt key no credentials cono initial send no port no ssh username Gradentials Fraction in the state of the stat	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
no aes encrypt key no credentials no initial send F no port no ssh username no tcp user timeout F Port crumbos	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.
no aes encrypt key no credentials Cono initial send For the series of th	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode cunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling.</number>
no aes encrypt key no credentials cono initial send no port no ssh username no tcp user timeout port <number> protocol ssh protocol ssl</number>	Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode cunneling. <number> = number of the port to use.</number>

protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:6:16) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:5:16) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent how digits. Bytes may run tegether or be congreted.

hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

enclose the value if it contains space Sets the connect tunnel AES encry 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. auto show statistics clrscrn enclose the value if it contains space 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. Show connection statistics Clears the screen.	pt key with up to by a single
aes encrypt key text <text> 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. auto show statistics clrscrn 16 bytes. Each byte is represented character. Note that quotes must er if it contains spaces. Show connection statistics Clears the screen.</text>	by a single
clrscrn Clears the screen.	
credentials <text> Selects the RSA/DSA certificates by SSL client.</text>	y name for the
default protocol Restores the default protocol as "To	CP".
default secure protocols Restores the default secure protocol	ol selections.
default tcp keep alive idle time Defaults the TCP keep alive idle time	ne.
default tcp keep alive interval Restores the default 45 second corkeep alive timeout.	nect mode TCP
default tcp keep alive probes Defaults the TCP keep alive probes	3.
exit Exits to the next higher level.	
Sets the host connect tunnel Initial allowing for binary characters. binary format that will be sent out the connection. Within [] use binary decorr hex up to 0xFF.	ary> = string in ne network upon
Sets the host connect tunnel Initial initial send set <text> = ascii string that will be sent out th connection.</text>	
no address Removes the remote host address tunneling connections.	used to establish
no aes decrypt key Removes the connect tunnel AES of	decrypt key.
no aes encrypt key Removes the connect tunnel AES e	encrypt key.
no credentials Clears the RSA/DSA certificate sele	ection.
no initial send Removes the host connect tunnel li	nitial Send string.
no port Removes the remote port used to e connections.	stablish tunnel
no ssh username Removes the SSH user name.	
no tcp user timeout Restores the default.	
port <number> Sets the remote port to use for contunneling. <number> = number of the</number></number>	
protocol ssh Uses SSH protocol for connect mod	de tunneling.
protocol ssl Uses SSL protocol for connect mod	
protocol tcp Uses TCP protocol for connect mod	
protocol tcp aes Uses TCP protocol with AES encry mode tunneling.	•
protocol telnet Uses Telnet protocol (with IAC) for tunneling.	connect mode
secure protocols ssl3 disable Disables the protocol.	
secure protocols ssl3 enable Enables the protocol.	
secure protocols tls1.0 disable Disables the protocol.	
secure protocols tls1.0 enable Enables the protocol.	
secure protocols tls1.1 disable Disables the protocol.	
secure protocols tls1.1 enable Enables the protocol.	

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 16 (tunnel-connect-host:4:16) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 16 (tunnel-connect-host:3:16) leve	l commands
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 16 (tunnel-connect-host:2:16) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 16 (tunnel-connect-host:1:16) level cor	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

	Outside d'accept fou TOD actions a d'actions
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 16 (config-host:16) level command	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 17 (config-host:17) level command	ls .
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.

protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 18 (config-host:18) level comma	ands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 19 (config-host:19) level comma	ands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
	P. · · · · · · ·
exit	Exits to the configuration level.

name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.		momory.
address < text> connections with. < text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is r	host 2 (tunnel-connect-host:16:2) level co	mmands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by with up to 12,3A,BC 12.3a.bc 12:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol default protocol selections.</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
aes decrypt key text < text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Clearacter. Note that quotes must enclose the value if it contains spaces. Selects Note that quotes must enclose the value if it contains spaces. Clears the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".	aes decrypt key <i><hexadecimal></hexadecimal></i>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key <hexadecimal> aes encrypt key <hexadecimal> by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics clrscrn credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol default secure protocols Restores the default secure protocol selections.</text></hexadecimal></hexadecimal>	aes decrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
aes encrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics clrscrn credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections.</text></text>	aes encrypt key <i><hexadecimal></hexadecimal></i>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
clrscrn Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol default secure protocols Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol as "TCP". Restores the default secure protocol selections.	aes encrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol default secure protocols Restores the default secure protocol selections.</text>	auto show statistics	show connection statistics
default protocol SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections.	clrscrn	Clears the screen.
default secure protocols Restores the default secure protocol selections.	credentials <text></text>	•
·	default protocol	Restores the default protocol as "TCP".
default tcp keep alive idle time Defaults the TCP keep alive idle time.	default secure protocols	Restores the default secure protocol selections.
	default tcp keep alive idle time	Defaults the TCP keep alive idle time.

default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,e.,,
host 2 (tunnel-connect-host:15:2) level (commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 2 (tunnel-connect-host:14:2) level comm	nands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

nds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:12:2) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 2 (tunnel-connect-host:11:2) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:10:2) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:9:2) level comm	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
	Uses Telnet protocol (with IAC) for connect mode
protocol telnet	tunneling.

secure protocols ist3.0 disable secure protocols ist3.1 disable secure protocols ist3.1 disable secure protocols ist3.1 disable secure protocols ist3.1 disable secure protocols ist3.2 disable secure protocol ist4.2 disable secure protocol ist5.2 disable secure protocol. Secure protocol ist5.2 disable secure protocol. Secure record. Secure protocol. Secure record. Secure protocol. Secure record. Secure		
secure protocols tis1.0 enable secure protocols tis1.1 disable secure protocols tis1.1 disable secure protocols tis1.2 disable secure protocols tis1.2 disable secure protocols tis1.2 enable secure protocols tis1.2 enable secure protocols tis1.2 enable Enables the protocol. secure protocols tis1.2 enable Enables the protocol. Secure protocols tis1.2 enable Enables the protocol. Secure protocol dy Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show support the secure to end tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interout. <milliseconds. <milliseconds="timer" <number="" alive="" and="" connect="" enables="" for="" in="" keep="" milliseconds.="" mode="" probes="" sets="" tcp="" the="" timer.="" tunneling="" value,=""> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12.3a BC*12.3a BC*12.3a bC *12.3a bC *12.</number></number></number></number></number></milliseconds.></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Jess with AES encryption for connect mode tunneling. Show show history Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <ext> = SSH user name. Sets the TCP keep alive idle time <milliseconds> step alive interval <milliseconds> step alive interval <milliseconds> top keep alive probes <number> step keep alive probes <number> step user timeout <milliseconds> step the timeout <milliseconds> step the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number =="" n<="" td=""><td>secure protocols tls1.0 disable</td><td>Disables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></ext>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show statistics Show statistics Show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time <milliseconds> tcp keep alive interval <milliseconds> cp user timeout <milliseconds> cp user timeout <milliseconds> step the palive probes <number> <te> sets the timer. milliseconds> = timer value, in milliseconds. Sets the TCP keep alive for connect mode tunneling and sets the timer. milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <number="" alive="" keep="" of="" probes.="" probes<="" tcp="" td=""><td>secure protocols tls1.0 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></te></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable Enables the protocol. Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show show statistics show connections statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> <mi>ctp keep alive probes </mi></milliseconds> <milliseconds. <milliseconds="" alive="" and="" connect="" enables="" for="" keep="" mode="" sets="" tcp="" the="" timer.="" tunneling=""> = timer value, in milliseconds> <mi>ctp user timeout <milliseconds> <milliseconds. (tunnel-connect-host:8:2)="" 2="" <hexadecimal="" aes="" alive="" certificate="" commands="" configuration="" connecting.="" current="" decrypt="" disable="" enable="" for="" in="" inst="" keep="" key="" level="" memory.="" number="" of="" permanent="" probes.="" retransmissions.="" server="" sets="" skips="" stores="" tcp="" the="" timeout="" validate="" verification="" when=""> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123AEC *12 3A BC* *12 3A BC*</text></milliseconds.></milliseconds></mi></milliseconds.></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol tish 1.2 enable protocol udp protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show Show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds = timeout value, in timeout value, in milliseconds = timeout value, in timeout value, in timeout value,</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes See UDP protocol for connect mode tunneling.	secure protocols tls1.2 disable	Disables the protocol.
protocol udp aes See UDP protocol for connect mode tunneling.	secure protocols tls1.2 enable	Enables the protocol.
show Shows the current configuration. Show history Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout of TCP retransmissions. <nilliseconds> = timeout value, in milliseconds. Validate certificate disable Validate certificate enable Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Fiost 2 (tunnel-connect-host:8:2) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12.3ABC "12</text></text></nilliseconds></number></number></milliseconds></milliseconds></text></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history show history show statistics show statistics show connection statistics show connection statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time. It is is the initial keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. validate certificate disable skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. It is a connection with server leading to the server certificate when connections. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12.3a,bc 12.3a;bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two indipects of the server. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two dijacent hex digits. Bytes may run together or be separated by two dijacent hex digits. Bytes may run together or be separated by two dijacent hex digits. Byte</number></number></number></milliseconds></milliseconds></text>	protocol udp aes	
show history show statistics show statistics show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <numbers (tunnel-connect-host-8-2)="" 2="" <numbers="number" <text="" =="" alive="" certificate="" commands="" configuration="" connecting.="" connections="" current="" disable="" enable="" establish="" host="" in="" keep="" level="" memory.="" nost="" number="" of="" permanent="" probes.="" remote="" requires="" server="" sets="" skips="" stores="" tcp="" the="" time="" to="" tunneling="" under="" validate="" verification="" when="" with.=""> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent he</numbers></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds. <milliseconds.="" <number="" alive="" and="" connect="" enables="" for="" keep="" mode="" number="" of="" probes.="" sets="" tcp="" the="" timer.="" tunneling=""> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate disable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. lost 2 (tunnel-connect-host:8:2) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 125a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text></milliseconds></number></milliseconds.></milliseconds></text>	show history	
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. rost 2 (tunnel-connect-host:8:2) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by a single character. Note that quotes must enclose the value if it contains spaces.</text></text></milliseconds></number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Post 2 (tunnel-connect-host:8:2) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC 12.33 bC 12.33 bC</text></text></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Tost 2 (tunnel-connect-host:8:2) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated</text></milliseconds></number></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. bost 2 (tunnel-connect-host:8:2) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by digits. Bytes may run together or be separated by the digits. Bytes may run together or be separated by digits.</text></text>	tcp keep alive probes < number>	
validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Nost 2 (tunnel-connect-host:8:2) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. **Nost 2 (tunnel-connect-host:8:2) level commands** address < text> Sets the remote host to establish tunneling connections with. < text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated	validate certificate disable	
memory. Nost 2 (tunnel-connect-host:8:2) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	write	
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text></text>	host 2 (tunnel-connect-host:8:2) level commands	
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>	aes decrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	
secure protocols tls1.1 enable	Disables the protocol. Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 2 (tunnel-connect-host:7:2) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Clears the schebyte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represen</text>		
address < text> connections with. < text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it by adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Clears the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".	host 2 (tunnel-connect-host:6:2) level con	nmands
aes decrypt key <hexadecimal> aes decrypt key <hexadecimal> by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.</hexadecimal></hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
aes decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics clrscrn Clears the screen. Credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".</text></text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key <hexadecimal> aes encrypt key <hexadecimal> aes encrypt key <hexadecimal> by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics clrscrn credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".</text></hexadecimal></hexadecimal></hexadecimal>	aes decrypt key text < text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
aes encrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics show connection statistics Clears the screen. Credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".</text></text>	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
clrscrn Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".	aes encrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
credentials <text> Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP".</text>	auto show statistics	show connection statistics
default protocol SSL client. Restores the default protocol as "TCP".	clrscrn	Clears the screen.
·	credentials <text></text>	•
default secure protocols Restores the default secure protocol selections.	default protocol	Restores the default protocol as "TCP".
	default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
·	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ls
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,
host 2 (tunnel-connect-host:4:2) level con	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
initial send set <text></text>	or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 2 (tunnel-connect-host:3:2) level command	S
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:2:2) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 2 (tunnel-connect-host:1:2) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 2 (config-host:2) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.

host <number></number>	Change to config host level
nama stayt	Sets the name of the host. <text> = name of the</text>
name <text></text>	host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 20 (config-host:20) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 21 (config-host:21) level commands	
clrscrn	Clears the screen.

default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address < text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 22 (config-host:22) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
	received the deladit value of the protector (remot).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected
·	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level.
exit host < <i>number</i> >	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the</text>
exit host <number> name <text></text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host.</text>
exit host <number> name <text> no name</text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host. Clears the name of the host.</text>
exit host <number> name <text> no name no remote address</text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host. Clears the name of the host. Clears the remote address of the host.</text>
exit host <number> name <text> no name no remote address no ssh username</text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host. Clears the name of the host. Clears the remote address of the host. Clears the SSH username associated with the host.</text>
exit host <number> name <text> no name no remote address no ssh username protocol ssh</text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host. Clears the name of the host. Clears the remote address of the host. Clears the SSH username associated with the host. Sets the protocol to SSH.</text>
exit host <number> name <text> no name no remote address no ssh username protocol ssh protocol telnet</text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host. Clears the name of the host. Clears the remote address of the host. Clears the SSH username associated with the host. Sets the protocol to SSH. Sets the IP address of the remote host to connect to when this host is selected on the login connect</text>
exit host <number> name <text> no name no remote address no ssh username protocol ssh protocol telnet remote address <text></text></text></number>	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol. Exits to the configuration level. Change to config host level Sets the name of the host. <text> = name of the host. Clears the name of the host. Clears the remote address of the host. Clears the SSH username associated with the host. Sets the protocol to SSH. Sets the protocol to Telnet. Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address. Sets the remote port used to connect to the host.</text></text>

show history

ssh username <text>

Displays the last 20 commands entered during the

Sets the username for logging into the host via

current CLI session.

SSH. <text> = username.

write	Stores the current configuration in permanent memory.
host 23 (config-host:23) level comma	nds
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 24 (config-host:24) level comma	nds
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>

show	Displays the current configuration.
	Displays the barrent commands entered during the
show history	current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 25 (config-host:25) level comma	ands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 26 (config-host:26) level comma	ands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.

remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 27 (config-host:27) level command	s
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 28 (config-host:28) level command	ls
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>

no nomo	Clears the name of the host.
no name no remote address	Clears the name of the flost. Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to 331. Sets the protocol to Telnet.
protocol temet	Sets the IP address of the remote host to connect to
remote address <text></text>	when this host is selected on the login connect menu. <text> = IP address.</text>
remote port < <i>number</i> >	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 29 (config-host:29) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:16:3) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>

aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
	Removes the remote port used to establish tunnel
no port	connections.
no port no ssh username	·
	connections.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:15:3) level command	ls .
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

character. Note intal quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the screen. Credentials <text> Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol as "TCP". default protocol Restores the default protocol as "TCP". default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second connect mode TCP keep alive interval keep alive interval keep alive interval hexep alive interval hexep alive interval hexep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel AES decrypt key. The protocol of the protocol of tunnel aes encrypt key. Removes the remote host address used to establish tunneling connections. Removes the remote host address used to establish tunneling connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port to use to connect mode tunneling. <br< th=""><th></th><th></th></br<></text>		
aes decrypt key text < text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12.3ABC*1* aes encrypt key **exadecimal** aes encrypt key text < text> Sets the connect tunnel AES encrypt key with up to 12,3A,BC*1* 12,3A,BC*12.3a.bc*12:3a:bc*Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel acceptance of the value if it contains spaces. Sets the RSA/DSA certificates by name for the SL client. default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second connect mode TCP keep alive timeout. Sets the default top keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary charactersbinarys = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0XFF. Sets the host connect tunnel Initial Send text. < text> = ascil string that will be sent out the network up		
16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Selects the RSA/DSA certificates by name for the SSL client. default protocol default protocol default protocol default secure protocols default top keep alive idle time default top keep alive idle time default top keep alive interval default top keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text>= assi string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES encrypt key. Removes the connect tunnel Initial Send string. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel Initial Send string. Removes the host connect tunnel Initial Send string. Removes the host connect tunnel Initial Send string. Removes the connect tunnel PES encrypt key. Removes the connec</text>	aes decrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
aes encrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics clrscrn Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols default tcp keep alive idle time Defaults the TCP keep alive idle time. Restores the default secure protocol selections. default tcp keep alive interval default tcp keep alive interval default tcp keep alive probes Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text. allowing for binary characters. Sets the host connect tunnel Initial Send text. asci string that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = asci string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the nost connect tunnel Initial Send string. Removes the host connect tunnel lating Send string. Removes the solution and Removes the connect tunnel Initial Send string. Removes the solution and Removes the fortunel Initial Send string. Removes the SSH user name. Removes the default. Sets the remote port used to establish tunnel connections. Removes the default. Sets the remote port to use for connect mode tunneling.</text></text>	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
Clears the screen. Credentials < text> Clears the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections. default top keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second connect mode TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. Initial send binary < binary> Sets the host connect tunnel Initial Send text allowing for binary characters. Initial send set < text> Sets the host connect tunnel Initial Send text allowing for binary characters. Initial send set < text> Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the sSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling.</text>	aes encrypt key text <text></text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. Defaults the TCP keep alive idle time Restores the default 45 second connect mode TCP keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default top keep alive probes Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. <a cinary"="" href="https://discrete/strings.new.new.new.new.new.new.new.new.new.new</td><td>auto show statistics</td><td>show connection statistics</td></tr><tr><td> SSL client. </td><td>clrscrn</td><td>Clears the screen.</td></tr><tr><td>default secure protocols Restores the default secure protocol selections. default to keep alive idle time Defaults the TCP keep alive idle time. default to keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default to keep alive probes Defaults the TCP keep alive probes. exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. -> string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text allowing for binary characters. -> binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. -> easii string that will be sent out the network upon connection. no address Removes the remote host address used to establish tunneling connections. no aes decrypt key Removes the connect tunnel AES decrypt key. no aes encrypt key Removes the connect tunnel AES encrypt key. no aes encrypt key Removes the connect tunnel Initial Send string. no port Removes the Post connect tunnel Initial Send string. no port Removes the SA/DSA certificate selection.	credentials <text></text>	
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling.</number></text>	default protocol	·
Restores the default 45 second connect mode TCP keep alive timeout. default tcp keep alive probes Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the FSH user name. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Port <number> protocol ssh Uses SSH protocol for connect mode tunneling.</number></text>		·
keep alive timeout. default tcp keep alive probes exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. solinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascil string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the remote host connect tunnel AES encrypt key. Removes the host connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the remote port used to establish tunnel connections. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the FSH user name. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Portocol ssh Uses SSL protocol for connect mode tunneling.</number></text>	default tcp keep alive idle time	·
Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. sinitial send binary binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling.</text>	default tcp keep alive interval	
Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the host connect tunnel Initial Send text allowing for binary characters. Sets the post connection. Within [] use binary decimal up to 255 or hex up to 0xFF.	default tcp keep alive probes	·
allowing for binary characters. allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh Uses SSH protocol for connect mode tunneling.</number></text>	exit	
= ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Protocol ssl Uses SSL protocol for connect mode tunneling.</number>	initial send binary binary>	allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255
tunneling connections. no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username no tcp user timeout port < number> protocol ssh ro aes decrypt key Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. < number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.	initial send set <text></text>	
no aes encrypt key no credentials Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Uses SSH protocol for connect mode tunneling.</number></number>	no address	Removes the remote host address used to establish tunneling connections.
no credentials no initial send Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssl Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Uses SSH protocol for connect mode tunneling.</number>	no aes decrypt key	7, 7
no initial send Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.</number>	no aes encrypt key	
Removes the remote port used to establish tunnel connections. no ssh username no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.</number></number>	no credentials	
connections. no ssh username no tcp user timeout port <number> protocol ssh rotocol ssl connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.</number></number>	no initial send	-
no tcp user timeout Port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.</number></number>	no port	connections.
port <number> Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.</number></number>	no ssh username	
protocol ssh protocol ssl tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.</number>	no tcp user timeout	
protocol ssl Uses SSL protocol for connect mode tunneling.	port <number></number>	·
	protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol tcp Uses TCP protocol for connect mode tunneling.	protocol ssl	·
	protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes Des TCP protocol with AES encryption for connect mode tunneling.		
secure protocols ssl3 disable secure protocols tls1.0 disable secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.1 disable Disables the protocol. Secure protocols tls1.2 disable Secure protocols tls1.2 disable Secure protocols tls1.2 disable Disables the protocol. Secure protocols tls1.2 disable Disables the protocol. Enables the protocol. Enables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show sthe current configuration. Show show the current configuration. Show statistics Show scannection statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for the protocol. Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may</milliseconds></mi></milliseconds></mi></milliseconds></milliseconds></text></text></text></text></text></text>	protocol tcp aes	
secure protocols sts10 enable secure protocols tis1.0 enable secure protocols tis1.0 enable secure protocols tis1.1 enable secure protocols tis1.1 enable secure protocols tis1.1 enable secure protocols tis1.2 enable secure protocol sit1.0 enable secure protocol. Secure protocol sit1.0 enable secure protocol. Secure protocol sit1.0 enable secure protocol. Secure protocol secure protocol sit1.0 enable secure protocol. Secure protocol sit1.0 enable secure protocol. Secure protocol secure protocol sit1.0 enable secure protocol secure protocol secure protocol sit1.0 enable secure protocol sit1.0 enable secure protocol sit1.0 enable secure protocol sit1.0 enable secure protocol secure protocol secure protocol sit1.0 enable secure protocol sit1.0 enable secure protocol secure pr	protocol telnet	· · · · · · · · · · · · · · · · · · ·
secure protocols tis1.0 disable secure protocols tis1.1 disable secure protocols tis1.2 disable Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> sets the time. This interval for the probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. Sets the connecting. Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the connect tunnel AES decrypt key with up to 15 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or b</number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Disables the protocol. secure protocols tls1.2 enable protocol udp protocol udp aes show Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> step keep alive probes <number> step user timeout <milliseconds> step user timeout of TCP keep alive probes. <number> step user timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Tost 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A, BC 12.3a, bc Note that quotes must enclose the value if it contains spaces.</text></number></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	secure protocols ssl3 enable	-
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Disables the protocol. secure protocols tls1.2 enable protocol udp protocol udp aes show Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> step keep alive probes <number> step user timeout <milliseconds> step user timeout of TCP keep alive probes. <number> step user timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Tost 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A, BC 12.3a, bc Note that quotes must enclose the value if it contains spaces.</text></number></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. dext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *123 AB C*123 ab C Note that quotes must enoble the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is fit contains spaces.</milliseconds></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp protocol udp protocol udp aes Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. text-> Sets the SSH user name for use when establishing tunneling connections with other devices. text-> Sets the TCP keep alive idle time. This is the initial keep alive interval mailtiseconds Enables TCP keep alive for connect mode tunneling and sets the timer. milliseconds top keep alive probes number> Sets the number of TCP keep alive probes. Sets the number of TCP keep alive probes. **Chumber> = number of TCP keep alive probes. **Sets the timeout for TCP retransmissions. **Illiseconds> = timeout value, in milliseconds. **Skips verification of the server certificate when connecting. **Skips verification of the server certificate when connecting. **Stores the current configuration in permanent memory. **Total (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <a **sets="" 12="" 12:3a,bc="" a<="" aes="" and="" connect="" contains="" decrypt="" enclose="" href="mailto: Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC " if="" it="" key="" must="" note="" quotes="" spaces.="" td="" that="" the="" to="" tunnel="" up="" value="" with=""><td>secure protocols tls1.1 disable</td><td>Disables the protocol.</td>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol stls1.2 enable protocol udp protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> step user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP terp ternamissions. <number> = number of TCP retainsisions. <number <number="number" =="" number="" of="" re<="" retainsisions.="" tcp="" td=""><td>secure protocols tls1.1 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
secure protocol stls1.2 enable protocol udp protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> step user timeout <milliseconds> Sets the number of TCP keep alive probes. <number> = number of TCP terp ternamissions. <number> = number of TCP retainsisions. <number <number="number" =="" number="" of="" re<="" retainsisions.="" tcp="" td=""><td>secure protocols tls1.2 disable</td><td>Disables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
protocol udp aes protocol udp aes show Show be current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show statistics show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top user timeout <milliseconds> step user timeout <milliseconds> step the meout <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds> = timer value, in milliseconds> = top user timeout <milliseconds> = top user timeout <milliseconds> = timer value, in milliseconds> = top user timeout <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds = timer value</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
show Show she current configuration. Shows the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. validate certificate disable validate certificate disable validate certificate enable validate certificate enable validate certificate enable validate certificate enable Sets the runner configuration in permanent memory. iost 3 (tunnel-connect-host:14:3) level commands Sets the runnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces.</number></milliseconds></milliseconds></milliseconds></milliseconds></text>	·	·
show history show history show statistics show statistics show connection statistics show connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> step user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate disable validate certificate enable validate certificate enable stores the current configuration in permanent memory. Fost 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 0.00 the value if it contains spaces.</text></milliseconds></number></number></number></number></number></milliseconds></number></milliseconds></milliseconds></text></text></text>		Uses UDP protocol with AES encryption for connect
show history show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. ctp user timeout <milliseconds> Sets the ineout for TCP retransmissions. <milliseconds> = timer value, in milliseconds = timeout value, in milliseconds. sets the number of TCP keep alive probes. ctp user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. validate certificate disable Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. validate certificate enable Stores the current configuration in permanent memory. rost 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 to 10</text></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show	-
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set she TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Tost 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 12:3ABC "12:3A BC" 12:3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive itmeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable validate certificate enable validate certificate enable stop user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Tost 3 (tunnel-connect-host:14:3) level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 24 contains spaces.</text></milliseconds></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. stores the current configuration in permanent memory. host 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. validate certificate disable validate certificate enable Stores the current configuration in permanent memory. **Nore the current configuration in permanent memory.* **Nore the current configuration in permanent memory. **Nore the current current configura</milliseconds></milliseconds></number></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate disable validate certificate enable write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 se</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. host 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 5. Sets the connect tunnel AES decrypt key with up to 5. Sets the connect tunnel AES decrypt key with up to 5.</text>	validate certificate disable	
memory. host 3 (tunnel-connect-host:14:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	validate certificate enable	· · · · · · · · · · · · · · · · · · ·
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	•
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 3 (tunnel-connect-host:14:3) level com	mands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	aes decrypt key text <text></text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols tls1.0 disable secure protocols tls1.1 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Secure protocols tls1.2 enable protocol udp Disables the protocol. Secure protocol tls1.2 enable protocol udp aes show Shows the current configuration. Shows the current configuration. Show shistory Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <a "12:3abc="" "12:3abc"="" 12:3abc="" 12:3abc"="" encoune="" href="https://doi.org/10.100/j.sch.100/</th><th></th><th><u> </u></th></tr><tr><td>secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Disables the protocol. secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show such current configuration. Shows the current configuration. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. ctext>= SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> ctp user timeout <milliseconds> ctp user timeout <milliseconds> sets the timeout for TCP keep alive probes. cumber> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the current configuration in permanent memory. Sets the current configuration in permanent free the set of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by two adjacen hex digits. Bytes may run together or be separated by two adjacen hex digits. Bytes may run together or be separated by the set of the set of the set of the set of the s</td><td>secure protocols ssl3 enable</td><td>Enables the protocol.</td></tr><tr><td>secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show statistics Show statistics show connection statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. ctext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> statistics statistics sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds = timer value, in milliseconds. Sets the number of TCP keep alive probes. Sets the inmout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable validate certificate enable sets the current configuration in permanent memory. Tost 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two diagreen hex digits. Bytes may run together or be separated by optional punctuation: 12:3ABC " memory.<="" must="" sendence="" td="" total=""><td>·</td><td>·</td>	·	·
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. secure protocol tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <te><te><te>SSH user namesh username <text>SSH user name for use when establishing tunneling connections with other devices. <te><te>SSH user namesh username <text>SSH user name for use when establishing tunneling connections with other devices. <te><te>SSH user namesh username <text>SSH user name for use when establishing tunneling connections with other devices. <te><te>sh user namesh username <te>SSH user name for use when establishing tunneling connections with other devices. <te><te>sh user namesh user nameSets the SSH user name for use when establishing tunneling connections with other devices. <te><te>sh user namesh user nameSets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.top keep alive interval <milliseconds>Sets the timer. <milliseconds> = timer value, in milliseconds.top user timeout <milliseconds>Sets the number of TCP keep alive probes.validate certificate disableSkips verification of the server certificate when connecting.validate certificate enableRequires verification of the server certificate when connecting.validate certificate enableSets the remote host to establish tunneling connections with. <te>Sets the connect tunnel AES decrypt key with up to 16</te></milliseconds></milliseconds></milliseconds></milliseconds></te></te></te></te></te></te></te></text></te></te></text></te></te></text></te></te></te>	·	·
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text>= SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> current CLI session. Sets the number of TCP keep alive probes. Sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> current configuration of the server certificate when connecting. validate certificate enable write Requires verification of the server certificate when connecting. Sets the connect of the server certificate when connecting. Sets the current configuration in permanent memory. Post 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12:3a.bc 12:3a.bc 12</text></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	·	·
secure protocols tls1.2 enable protocol udp protocol udp protocol udp protocol udp ass Show Show secure tronginguration. Show show history Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds. <milliseconds="" alive="" interval="" keep="" top=""> top keep alive probes <number> top keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <number="" alive="" keep="" of="" probes.="" tc<="" tcp="" td=""><td>secure protocols tls1.1 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></milliseconds.></text></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp protocol udp aes show show Shows the current configuration. Show statistics Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> step user timeout <milliseconds> top user timeout <milliseconds> sets the timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. Sets the timeout value, in milliseconds. Sets the timeout for TCP retransmissions. Sets the connecting. Sets the connecting. Sets the connecting. Sets the connecting. Sets the connecting the time the time</milliseconds></milliseconds></number></number></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
Uses UDP protocol with AES encryption for connermode tunneling. Show Show Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, ir milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top user timeout <milliseconds> sets the timeout for TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Validate certificate enable Validate cer</milliseconds></number></number></milliseconds></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
show Shows the current configuration. Show history Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial top keep alive idle time <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> sets the number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the timeout for TCP retransmissions. smilliseconds> = timeout for TCP retransmissions. smilliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. smilliseconds> = timeout value, in milliseconds. Validate certificate disable skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Itost 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to the features of the server of the s</text></number></number></milliseconds></milliseconds></milliseconds></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text></text>	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show statistics show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunnelin and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number <number="" alive="" alive<="" keep="" of="" probes.="" tcp="" td=""><td>show</td><td>Shows the current configuration.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive initial keep alive idle time. This is the initial keep alive intended. Enables TCP keep alive for connect indeep alive probes. Sets the number of TCP keep alive probes. Sets the timeout of TC</text>	show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive itimeout. <milliseconds> = timer value, ir milliseconds. Enables TCP keep alive for connect mode tunnelin and sets the timer. <milliseconds> = timer value, ir milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number <number="" <text="" alive="" configuration="" connections="" current="" establish="" for="" host="" in="" keep="" memory.="" of="" permanent="" probes.="" remote="" retransmissions.="" sets="" stores="" tcp="" the="" timeout="" to="" tunneling="" with.=""> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes musenclose the value if it contains spaces.</number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, ir milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, ir milliseconds> tcp keep alive probes <number> tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Nost 3 (tunnel-connect-host:13:3) level commands** Sets the remote host to establish tunneling connections with. <lext> = IP address or host namof the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</lext></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	SSH user name.
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp user timeout <milliseconds> tcp user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Inost 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text></milliseconds></number></milliseconds></milliseconds></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	
connections with. 	tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Nost 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text>	tcp keep alive probes < number>	
validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. host 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text>	validate certificate disable	
host 3 (tunnel-connect-host:13:3) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text>	write	,
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</text>	host 3 (tunnel-connect-host:13:3) level command	ds
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacen hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes mus enclose the value if it contains spaces.</hexadecimal>		Sets the remote host to establish tunneling connections with. <text> = IP address or host name</text>
Sets the connect tunnel AES decrypt key with up to	aes decrypt key <i><hexadecimal></hexadecimal></i>	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes decrypt key text < text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.	aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
16 bytes. Each byte is represented by two adjacen	aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 3 (tunnel-connect-host:12:3) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 3 (tunnel-connect-host:11:3) level	commands
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 3 (tunnel-connect-host:10:3) level command	ls
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,
host 3 (tunnel-connect-host:9:3) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

<text>upon stablish y. y. string. unnel</text>
y. y. string. innel
string.
string.
string.
innel
use.
ng.
g.
ıg.
onnect
ode
ng.
onnect
g the
ishing xt> =
initial lue, in
nneling
ue, in
i

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:7:3) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
	Removes the remote port used to establish tunnel
no port	connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 3 (tunnel-connect-host:6:3) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect
protocol top aes	mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:5:3) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:4:3) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
	Uses Telnet protocol (with IAC) for connect mode
protocol telnet	tunneling.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:3:3) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 3 (tunnel-connect-host:2:3) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	inemory.
host 3 (tunnel-connect-host:1:3) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 3 (config-host:3) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 30 (config-host:30) level commands	
cirscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.

host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the</text>
no name	host. Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address < text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 31 (config-host:31) level comm	nands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.
host 32 (config-host:32) level comm	nands
clrscrn	Clears the screen.

default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address < text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:16:4) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.

credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:15:4) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols default tcp keep alive idle time	Restores the default secure protocol selections. Defaults the TCP keep alive idle time.

default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	, ,
host 4 (tunnel-connect-host:14:4) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <pre><milliseconds> = timeout value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	, y
host 4 (tunnel-connect-host:13:4) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection Within Dans Lines desired at 6.055
	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

nds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:11:4) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:10:4) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:9:4) level comm	nands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	
	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections.
no aes decrypt key	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key.
no aes decrypt key no aes encrypt key	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key.
no aes decrypt key no aes encrypt key no credentials	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection.
no aes decrypt key no aes encrypt key	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string.
no aes decrypt key no aes encrypt key no credentials	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.
no aes decrypt key no aes encrypt key no credentials no initial send no port	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name.
no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username no tcp user timeout port <number> protocol ssh</number>	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number> Uses SSH protocol for connect mode tunneling.
no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username no tcp user timeout port <number></number>	 ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>

protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling.		
secure protocols ssl3 disable secure protocols ssl3 enable secure protocols ssl3 enable secure protocols tsl1.0 disable secure protocols tsl1.0 enable secure protocols tsl1.1 denable secure protocols tsl1.2 disable secure protocols tsl1.2 disable secure protocols tsl1.2 denable Enables the protocol. secure protocols tsl1.2 denable Enables the protocol. Secure protocols tsl1.2 denable Enables the protocol. Secure protocols tsl1.2 enable Enables the protocol. Secure protocol stl1.2 denable Enables the protocol. Secure protocol. Secure protocols tsl1.2 denable Enables the protocol. Secure protocol. Secure protocols tsl1.2 denable Enables the protocol. Secure protocol. Secure protocol. Secure protocol stl1.2 denable Enables the protocol. Secure protocol. Secure protocol. Secure protocol. Secure protocol stl1.2 denable Secure protocol. Secure pr	protocol tcp aes	•
secure protocols ss13 enable secure protocols ts10. disable secure protocols ts10. disable secure protocols ts10. denable secure protocols ts11.1 disable Disables the protocol. secure protocols ts11.1 disable Disables the protocol. Secure protocols ts11.2 disable Disables the protocol. Secure protocols ts11.2 disable Disables the protocol. Secure protocols ts11.2 enable Secure protocols ts11.2 enable Disables the protocol. Secure protocol ts11.2 enable Disables the protocol. Secure protocol ts11.2 enable Disables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> tcp keep alive interval <milliseconds> sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number certificate="" connec<="" of="" server="" td="" the="" when=""><td>protocol telnet</td><td>, ,</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></text>	protocol telnet	, ,
secure protocols ss13 enable secure protocols ts10. disable secure protocols ts10. disable secure protocols ts10. denable secure protocols ts11.1 disable Disables the protocol. secure protocols ts11.1 disable Disables the protocol. Secure protocols ts11.2 disable Disables the protocol. Secure protocols ts11.2 disable Disables the protocol. Secure protocols ts11.2 enable Secure protocols ts11.2 enable Disables the protocol. Secure protocol ts11.2 enable Disables the protocol. Secure protocol ts11.2 enable Disables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> tcp keep alive interval <milliseconds> sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number certificate="" connec<="" of="" server="" td="" the="" when=""><td>secure protocols ssl3 disable</td><td></td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols ssl3 disable	
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocol tls1.2 enable secure protocol. Secure to protocol. Secure tlast protocol. Secure to protocol. Secure titles and secure titles and secure to protocol. Secure titles and secure titles. Secure titles protocol. Secure titles protocol. Secure titles	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocol tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundbers = number of TCP keep alive probes. cundb</milliseconds></milliseconds></text>	secure protocols tls1.0 disable	Disables the protocol.
Enables the protocol. Secure protocols tls1.2 disable Secure protocols tls1.2 disable Secure protocols tls1.2 disable Protocol udp Disables the protocol. Uses UDP protocol for connect mode tunneling, Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show as UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> top keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. Sets the timeout value, in milliseconds> willidate certificate disable Sets the timeout value, in milliseconds. Skips verification of the server certificate when connecting. Williaconds> = timer value, in milliseconds> Requires verification of the server certificate when connecting. Sets the timeout value, in milliseconds. Skips verification of the server certificate when connecting. Sets the connect tunnel AES decrypt key when one of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A BC "12.3A BC" 12.3A BC "12.3A BC" 12.3A BC "12.3A BC" 12.3A BC "12.3A BC" 12.3A B</number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocol tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> step alive interval <milliseconds> top keep alive interval <milliseconds> sets the timer. <milliseconds> = timer value, in milliseconds. Top keep alive probes <number> sets the timer. <milliseconds> = timer value, in milliseconds. Sets the timeout for TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <number> = number of TCP</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
Enables the protocol. Uses UDP protocol for connect mode tunneling. Protocol udp aes Show Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> Sets the number of TCP keep alive probes. <numbers <milliseconds="" =="" alive="" keep="" mount="" number="" of="" or="" probes.="" retransmissions.="" sets="" tcp="" the=""> = time value, in milliseconds> = time value, in milliseconds = time value, in milliseconds. Sets the number of TCP keep alive probes. <multiple conds<="" mi=""> Sets the number of TCP keep alive probes. <multiple conds<="" mi=""> Sets the number of TCP keep alive probes. <multiple conds<="" mi=""> Sets the timeout for TCP retransmissions. <multiple conds<="" mi="" multiple=""> Sets the timeout for TCP retransmissions. <multiple conds<="" mi="" multiple=""> Sets the timeout for TCP retransmissions. <multiple conds<="" mi="" multiple=""> Sets the timeout for TCP retransmissions. <multiple conds<="" multiple="" td=""><td>secure protocols tls1.1 enable</td><td>Enables the protocol.</td></multiple></multiple></multiple></multiple></multiple></multiple></multiple></numbers></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes protocol udp aes show Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. stop user timeout <milliseconds> stop user timeout connecting. Sets the number of TCP keep alive probes. squilidate certificate disable validate certificate disable validate certificate enable Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 spaces. Sets the connect tunnel AES decrypt key with up to 10 spaces. Sets the connect tunnel AES decrypt key with up to 10 spaces. Sets the connect tunnel AES decrypt key with up to 10 spaces. Sets the connect tunnel AES decrypt key with up to 10 spaces. Sets the connect tunnel AES decrypt key with</text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></text></text>	secure protocols tls1.2 disable	Disables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = temer value, in milliseconds. Exp keep alive probes <number> = number of TCP keep alive probes. <number <number="" alive="" keep="" keep<="" of="" probes.="" tcp="" td=""><td>secure protocols tls1.2 enable</td><td>Enables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout, <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host 8:4) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces.</text></text></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history show statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices, stext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. Most 4 (tunnel-connect-host:8:4) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10.6 bytes. Each byte that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc 12.3a.bc Note that quotes must enclose the value if it contains spaces.</text></text></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	protocol udp aes	
show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a. bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 and 10 and</text></text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds. <number="" =="" alive="" in="" keep="" milliseconds.="" probes="" tcp="" timer="" value,=""> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></number></number></milliseconds.></milliseconds></text>	show history	
tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text></milliseconds></milliseconds></number></milliseconds></milliseconds></milliseconds></text>	show statistics	show connection statistics
keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> top keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. top user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <lext> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3a, BC 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2 sets the connect tunnel AES decrypt key with up to 2 sets the value if it contains spaces.</lext></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
and sets the timer. <milliseconds> = timer value, in milliseconds. top keep alive probes <number> top keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8;4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></number></number></number></number></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
conumber> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. smilliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to Sets the connect tunnel AES decrypt key with up to</text></milliseconds>	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
cp user timeout <milliseconds> smilliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to Sets the connect tunnel AES decrypt key with up to</text></milliseconds>	tcp keep alive probes <number></number>	
validate certificate enable validate certificate enable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp user timeout <milliseconds></milliseconds>	
connecting. Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 5 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key with up to 6 sets the connect tunnel AES decrypt key wi</text>	validate certificate disable	
memory. host 4 (tunnel-connect-host:8:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	· · · · · · · · · · · · · · · · · · ·
connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	host 4 (tunnel-connect-host:8:4) level com	
16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <i><hexadecimal></hexadecimal></i>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	aes decrypt key text <text></text>	

	abarastar Nata that quates recet englace the colors
	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols tst3.0 disable secure protocols tst3.1 disable secure protocols tst3.1 disable secure protocols tst3.1 disable secure protocols tst3.1 disable secure protocols tst3.2 disable secure protocol tst3.2 disable secure protocol. Secure record tital. Secure commands entered during the current Culession. Sets the TCP keep alive our set when establishing and sets the timer. Sets the timeoutmilliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timermilliseconds> = timer value, in milliseconds> sets the timent. of TCP keep alive probesnumber of T		
secure protocols tis1.0 enable secure protocols tis1.1 disable secure protocols tis1.1 disable secure protocols tis1.2 disable secure protocols tis1.2 disable secure protocols tis1.2 enable secure protocols tis1.2 enable secure protocols tis1.2 enable secure protocols tis1.2 enable Enables the protocol. secure protocol dip Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show connection statistics show connection statistics show connection statistics show connection statistics show the current configuration. Displays the last 20 commands entered during the current CLI session. show with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idel time. This is the initial keep alive idel time. This is the initial keep alive interval <milliseconds. <milliseconds="" alive="" and="" connect="" enables="" for="" keep="" mode="" sets="" tcp="" the="" timer.="" tunneling=""> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. Validate certificate enable Sets the remote host to establish tunneling connections with, <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Se</text></number></number></number></number></number></milliseconds.></text></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <table 4<="" length="" td=""><td>secure protocols tls1.0 disable</td><td>Disables the protocol.</td></table>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show statistics Show statistics Show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name SSH user name. Sets the TCP keep alive idle time *milliseconds> stop keep alive interval *milliseconds> top keep alive probes *number> top keep alive probes *number> stop user timeout *milliseconds> stop user timeout *millisecon</text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable Secure protocols tls1.2 enable Enables the protocol. Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connections statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> <milliseconds> = timer value, in milliseconds> <milliseconds. <milliseconds="" alive="" keep="" number="" of="" probes.="" sets="" tcp="" the=""> = timer value, in milliseconds> <milliseconds> = timer value, in milliseconds> <milliseconds> = timer value, in milliseconds> <milliseconds> = timeout value, in milliseconds> <milliseconds> = timeo</milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds.></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol tidp	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes Uses UDP protocol for connect mode tunneling.	secure protocols tls1.2 disable	Disables the protocol.
protocol udp aes Uses UDP protocol for connect mode tunneling.	secure protocols tls1.2 enable	Enables the protocol.
show Show show the current configuration. Show history Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive interval <milliseconds></milliseconds></text></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history show history show statistics show connection statistics show connection statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. solution of TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <number> = number of TCP keep alive probes. Sets the connecting. Stores the current configuration in permanent memory. Inst 4 (tunnel-connect-host-7-4) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by volutional spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated by</number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	protocol udp aes	
show history Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <numbers <milliseconds="" <numbers="number" =="" alive="" keep="" number="" of="" probes.="" tcp=""> = timer value, in milliseconds> = timer value, in milliseconds. Sets the invent for TCP retransmission. <milliseconds. <milliseconds=""> = timeout value, in milliseconds. <milliseconds> = timeout value, in milliseconds = timeout value, in milliseconds = timer value, in milliseconds = timer value, in milliseconds. <milliseconds =="" in="" milliseconds="timer" milliseconds<="" td="" timer="" value,=""><td>show</td><td>Shows the current configuration.</td></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds.></numbers></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time <milliseconds> to milliseconds> to milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds. (tunnel-connect-host:7:4)="" 4="" <milliseconds="timeout" <multiple="" <text="" alive="" and="" certificate="" commands="" conders="number" configuration="" connect="" connecting.="" connections="" current="" disable="" enable="" enables="" establish="" for="" host="" in="" keep="" level="" memory.="" milliseconds.="" mode="" nost="" number="" of="" permanent="" probes.="" remote="" requires="" retransmissions.="" server="" sets="" skips="" stores="" tcp="" the="" timeout="" timer.="" to="" tunneling="" validate="" value,="" verification="" when="" with.=""> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by 50 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by 50 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</milliseconds.></milliseconds></text>	show history	
ssh username <text> tunneling connections with other devices. <text> = SSH user name. Set sthe TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number></number></milliseconds></milliseconds></text></text>	show statistics	show connection statistics
tcp keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> tcp user timeout <milliseconds> tcp user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Post 4 (tunnel-connect-host:7:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC 12.33 bC 12.33 bC 12.33 bC 12.33 bC 12.33 bC Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by sets here one tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by sets here one tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by sets here one or be separated by two adjacent hex digits. Bytes may run together or be separated</text></milliseconds></number></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. **Nost 4 (tunnel-connect-host:7:4) level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated</text></milliseconds></number></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 4 (tunnel-connect-host:7:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	tcp keep alive probes < number>	
validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Nost 4 (tunnel-connect-host:7:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by two adjacent hex digits. Bytes may run together or be separated</text>	tcp user timeout <milliseconds></milliseconds>	
write Stores the current configuration in permanent memory. **Nost 4 (tunnel-connect-host:7:4) level commands** address < text> Sets the remote host to establish tunneling connections with. < text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated	validate certificate disable	
memory. Nost 4 (tunnel-connect-host:7:4) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	validate certificate enable	
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	write	
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text></text>	host 4 (tunnel-connect-host:7:4) level commands	
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated</hexadecimal>	aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:6:4) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,
host 4 (tunnel-connect-host:5:4) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:4:4) level con	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:3:4) level com	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:2:4) level comma	nds
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:1:4) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel
	connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 4 (config-host:4) level commands

clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

host 5 (tunnel-connect-host:16:5) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics

clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 5 (tunnel-connect-host:15:5) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

•
ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 5 (tunnel-connect-host:13:5) level (commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

Sets the host connect tunnel Initial Send to a sci string that will be sent out the network connection. Removes the remote host address used to tunneling connections. Removes the connect tunnel AES decrypt no aes encrypt key Removes the connect tunnel AES encrypt no credentials Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send Removes the host connect tunnel Initial Send Removes the remote port used to establish connections. Removes the remote port used to establish connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunnel protocol ssh Uses SSH protocol for connect mode tunnel protocol tcp Uses TCP protocol for connect mode tunnel protocol tcp aes	
no address tunneling connections. no aes decrypt key no aes encrypt key no credentials no initial send no port no ssh username no tcp user timeout port <number> port <number> port <number> port cocol ssh protocol ssl protocol tcp protocol tcp ro aes encrypt key Removes the connect tunnel AES encrypt Removes the RSA/DSA certificate selection. Removes the host connect tunnel Initial Selection. Removes the remote port used to establish connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port Uses SSL protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling.</number></number></number></number>	
no aes encrypt key no credentials Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Set no port Removes the remote port used to establish connections. no ssh username Removes the SSH user name. Restores the default. Sets the remote port to use for connect me tunneling. <number> = number of the port protocol ssh Uses SSH protocol for connect mode tunnel protocol tcp Uses TCP protocol with AES encryption for</number>	o establish
no credentials no initial send Removes the host connect tunnel Initial Set Removes the remote port used to establish connections. no ssh username Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port protocol ssh protocol ssl protocol ssl protocol tcp Uses TCP protocol with AES encryption for</number>	key.
no credentials no initial send Removes the host connect tunnel Initial Set Removes the remote port used to establish connections. no ssh username Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port protocol ssh Protocol ssl Uses SSL protocol for connect mode tunneling. Sets TCP protocol with AES encryption for</number>	key.
no port Removes the remote port used to establish connections. no ssh username Removes the SSH user name. Restores the default. Sets the remote port to use for connect more tunneling. <number> = number of the port unneling. <number <number="" of="" port="" td="" the="" unnelin<="" unneling.=""><td></td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number>	
no ssh username no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port protocol ssh protocol ssl protocol tcp Uses TCP protocol with AES encryption for</number></number>	end string.
no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port Uses SSH protocol for connect mode tunneling. protocol tcp Uses TCP protocol with AES encryption for</number></number>	h tunnel
port <number> Sets the remote port to use for connect mot tunneling. <number> = number of the port unneling. <number> = number of the port unneling. <number> = number of the port unneling. <number> = number of the port unnel unn</number></number></number></number></number>	
port <number> Sets the remote port to use for connect mot tunneling. <number> = number of the port unneling. <number> = number of the port unneling. <number> = number of the port unnel u</number></number></number></number>	
protocol ssl Uses SSL protocol for connect mode tunn protocol tcp Uses TCP protocol for connect mode tunn Uses TCP protocol with AES encryption for	
protocol tcp Uses TCP protocol for connect mode tunn Uses TCP protocol with AES encryption for	neling.
Uses TCP protocol with AES encryption for	eling.
	neling.
mode tunneling.	or connect
protocol telnet Uses Telnet protocol (with IAC) for connect tunneling.	ct mode
secure protocols ssl3 disable Disables the protocol.	
secure protocols ssl3 enable Enables the protocol.	
secure protocols tls1.0 disable Disables the protocol.	
secure protocols tls1.0 enable Enables the protocol.	
secure protocols tls1.1 disable Disables the protocol.	
secure protocols tls1.1 enable Enables the protocol.	
secure protocols tls1.2 disable Disables the protocol.	
secure protocols tls1.2 enable Enables the protocol.	
protocol udp Uses UDP protocol for connect mode tunn	neling.
protocol udp aes Uses UDP protocol with AES encryption for mode tunneling.	or connect
show Shows the current configuration.	
show history Displays the last 20 commands entered du current CLI session.	uring the
show statistics show connection statistics	
Sets the SSH user name for use when est tunneling connections with other devices. SSH user name.	_
Sets the TCP keep alive idle time. This is to keep alive idle time <milliseconds> tcp keep alive idle time <milliseconds> = timer milliseconds.</milliseconds></milliseconds>	
tcp keep alive interval <milliseconds> Enables TCP keep alive for connect mode and sets the timer. <milliseconds> = timer milliseconds.</milliseconds></milliseconds>	value, iii
tcp keep alive probes < <i>number></i> Sets the number of TCP keep alive probes < <i>number></i> = number of TCP keep alive probes	e tunneling

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 5 (tunnel-connect-host:12:5) level comman	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:11:5) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 5 (tunnel-connect-host:2:5) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:9:5) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Secure protocols sts1.0 disable Secure protocols tts1.0 disable Secure protocols tts1.1 disable Secure protocols tts1.1 disable Secure protocols tts1.1 disable Secure protocols tts1.1 disable Secure protocols tts1.2 disable Secure protocol tts1.2 disable Secure protocol tts1.2 disable Secure protocol usp Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = \$\$SH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout, cmilliseconds> = timer value, in milliseconds> tcp keep alive probes <number> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> Sets the timeout for TCP keep alive probes. Sets the timeout for TCP keep alive probes. Sets the immeut of TCP keep alive probes. Sets the immeut of the server certificate when connecting. Write Sets the current configuration in permanent memory. Nost 5 (tunnel-connect-host/8:5) level commands Sets the rome host to establish tunneling connections with. <te> text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *123ABC* 123ABC* 123ABC* 123ABC* 123ABC* 123ABC* 123ABC* 123ABC* 123ABC* 124BC* 124BC* 124BC* 124BC* 124BC* 124BC* 124BC* 124BC* 124BC* 12</te></milliseconds></number></text>		
secure protocols ssl3 disable secure protocols ssl3 enable Secure protocols ssl3.0 enable Secure protocols tls1.0 enable Secure protocols tls1.1 enable Secure protocols tls1.2 disable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol tls1.2 enable Disables the protocol. Enables the protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Enables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Secure protocol tls1.2 enable Disables the protocol. Secure protocol. Secure protocol tls1.2 enable Disables the protocol. Secure protocol the secure during the current configuration of the server certificate when connecting. Sets the connect tinnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 1243ABC 1/2 aABC 1/2 aABC 1/2 aABC 1/2 aABC 1	protocol tcp aes	
secure protocols sts10 enable secure protocols tst1.0 disable secure protocols tst1.0 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.2 disable Secure protocols tst1.2 enable Secure protocols tst1.2 enable Secure protocols tst1.2 enable Secure protocols tst1.2 enable Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds tcp keep alive probes <number> scape and sets the timer. <milliseconds> = timer value, in milliseconds> sets the mumber of TCP keep alive probes. <number> = number of TCP keep alive probes. <number of="" td="" the<=""><td>protocol telnet</td><td>· · · · · · · · · · · · · · · · · · · ·</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></text>	protocol telnet	· · · · · · · · · · · · · · · · · · · ·
secure protocols sts10 enable secure protocols tst1.0 disable secure protocols tst1.0 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.1 enable secure protocols tst1.2 disable Secure protocols tst1.2 enable Secure protocols tst1.2 enable Secure protocols tst1.2 enable Secure protocols tst1.2 enable Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds tcp keep alive probes <number> scape and sets the timer. <milliseconds> = timer value, in milliseconds> sets the mumber of TCP keep alive probes. <number> = number of TCP keep alive probes. <number of="" td="" the<=""><td>secure protocols ssl3 disable</td><td>Disables the protocol.</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></number></milliseconds></text>	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp protocol udp protocol udp aes show Show show show show show istory show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> step keep alive probes <number> step user timeout <milliseconds> step timeout split user of TCP keep alive probes. <mi>milliseconds> = timeout value, in milliseconds. step user timeout <milliseconds> step timeout value, in milliseconds. steps verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. Tost 5 (tunnel-connect-host 8:5) level commands Sets the remote host to establish tunneling connections with . text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12.3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</milliseconds></mi></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></milliseconds></text>	secure protocols ssl3 enable	•
secure protocols tls1.1 disable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocol tldp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds <number="" =="" alive="" in="" keep="" milliseconds.="" probes="" tcp="" timer="" value,=""> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> number of TCP ke</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 disable	·
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show bistory Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <number> = n</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Disables the protocol. Secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <tp>sets the number of TCP keep alive probes. sets the mumber of TCP keep alive probes. sets the mumber of TCP keep alive probes. sets the timeout <milliseconds> sets the timeout for TCP retransmissions. sets the timeout for TCP retransmissions. sets the timeout of TCP retransmissions. sets the timeout of TCP retransmissions. sets the timeout for TCP retransmissions. sets the server certificate when connecting. Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12.3a.bc *12.3</text></milliseconds></tp></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol sts1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. squildate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. Post 5 (tunnel-connect-host:8-5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 12 sa,bc 12:3a,bc 1</text></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
secure protocol sts1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. squildate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. Post 5 (tunnel-connect-host:8-5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 10 sets the connect tunnel AES decrypt key with up to 12 sa,bc 12:3a,bc 1</text></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. **stillseconds** = timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the remote for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the connecting. Sets the current configuration in permanent memory. **Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. **Requires verification of the server certificate when connections with <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hox digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bC 12.3a,bC Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 to 10</text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling.	·	•
Show statistics show statistics show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time <milliseconds> top keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> top user timeout <milliseconds> Sets the timeout for TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the number of TCP retransmissions. <number> = number of the server certificate when connecting. Skips verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Inst 5 (tunnel-connect-host:8:5) level commands aeddress <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 to 12 to</text></text></number></number></number></number></number></number></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>		Uses UDP protocol with AES encryption for connect
show history Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Most 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 10.2:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 and 10</text></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set she TCP keep alive idle time. This is the initial keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. host 5 (tunnel-connect-host:3:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the
tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></text>	show statistics	show connection statistics
keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123ABC" 123ABC 123a.bc 123a.bc 123a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. validate certificate disable Skips verification of the server certificate when connecting. validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 23 and 23 are connected and 24 are connected and 25 ar</text></milliseconds></milliseconds></number></number></number></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate enable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 sets the connect tunnel AES decrypt</text>	tcp user timeout <milliseconds></milliseconds>	
vrite Stores the current configuration in permanent memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 sets the connect tun</text>	validate certificate disable	
memory. host 5 (tunnel-connect-host:8:5) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 2 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text> Sets the connect tunnel AES decrypt key with up to 3 decrypt key text < text</text>	validate certificate enable	· •
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	,
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 5 (tunnel-connect-host:8:5) level comm	mands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
	aes decrypt key text <text></text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tis1.0 enable	Enables the protocol.
secure protocols tIs1.1 disable	Disables the protocol.
secure protocols tIs1.1 enable	Enables the protocol.
secure protocols tIs1.2 disable	Disables the protocol.
secure protocols tis1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol dup	Uses UDP protocol with AES encryption for connect
protocol udp aes	mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:7:5) level command:	5
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

hart E (tunnal connect hastifies) lovel commands	
host 5 (tunnel-connect-host:6:5) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 5 (tunnel-connect-host:5:5) level comm	nands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 5 (tunnel-connect-host:4:5) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	, ,
host 5 (tunnel-connect-host:3:5) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

nds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:1:5) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel
	connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 5 (config-host:5) level commands

cirscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:16:6) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics

clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 6 (tunnel-connect-host:15:6) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,e.,,
host 6 (tunnel-connect-host:14:6) level of	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:13:6) level comman	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection Within Duce himery desired on to OFF
	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:12:6) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

Removes the remote host address used to establish tunneling connections.
Removes the connect tunnel AES decrypt key.
Removes the connect tunnel AES encrypt key.
Clears the RSA/DSA certificate selection.
Removes the host connect tunnel Initial Send string.
Removes the remote port used to establish tunnel connections.
Removes the SSH user name.
Restores the default.
Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
Uses SSH protocol for connect mode tunneling.
Uses SSL protocol for connect mode tunneling.
Uses TCP protocol for connect mode tunneling.
Uses TCP protocol with AES encryption for connect mode tunneling.
Uses Telnet protocol (with IAC) for connect mode tunneling.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Disables the protocol.
Enables the protocol.
Uses UDP protocol for connect mode tunneling.
Uses UDP protocol with AES encryption for connect mode tunneling.
Shows the current configuration.
Displays the last 20 commands entered during the current CLI session.
show connection statistics
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:11:6) level (commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
•	Sets the remote port to use for connect mode
port <number></number>	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:10:6) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:9:6) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:8:6) level com	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:7:6) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

aes encrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics show connection statistics cIrscrn Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default top keep alive idle time Defaults the TCP keep alive idle time. default top keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default top keep alive probes Defaults the TCP keep alive probes. exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. </text>		12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key text < lext> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics show connection statistics clears the screen. Clears the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default ttop keep alive idle time Defaults the TCP keep alive idle time. default top keep alive interval Restores the default 45 second connect mode TCP keep alive probes Defaults the TCP keep alive probes. Exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. cbinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. < exchange in the network upon connection. no address initial send set Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no ase decrypt key no ase encrypt key no ase sencrypt key no ase sencrypt key no eredentials No credentials Removes the connect tunnel Initial Send string encounted the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the host connect tunnel Initial Send string encounted the network upon connections. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the host connect tunnel Initial Send string encounted the network upon connections. Removes the femole port used to establish tunnel connections. Removes the forting in the port to use for connect mode tunneling. Uses SSL protocol for connect		·
Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default tcp keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second connect mode TCP keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default tcp keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default tcp keep alive probes Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters, chinary> string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text: <number="" address="" aes="" ascii="" be="" certificate="" clears="" connect="" connection.="" connections.="" decrypt="" default.="" dort="" dsa="" encrypt="" establish="" host="" initial="" key.="" nest="" network="" out="" port="" remote="" removes="" restores="" rsa="" selection.="" send="" sent="" string="" that="" the="" to="" tunnel="" tunneling="" upon="" used="" will=""> Removes the remote port to use for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp Uses SSL protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Protocol telnet SECURD Protocol (with IAC) for connect mode tunneling. Disables the protocol. Disables the protocol. Disables the protocol.</text:>	aes encrypt key text <text></text>	character. Note that quotes must enclose the value
Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections. Restores the default secure protocol. Restores the default. Res	auto show statistics	show connection statistics
default protocol default secure protocols default secure protocols default secure protocols default to keep alive idle time default top keep alive idle time default top keep alive interval default top keep alive interval default top keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characterschinary> = string in initial send binary -binary> binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text, -text: = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no ase decrypt key no ase encrypt key no ase encrypt key no ase encrypt key no are dentials Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling, orunmber> protocol ssh Uses SSL protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Protocol top Uses TCP protocol (with IAC) for connect mode tunneling. Protocol telnet Secure protocols tis1.0 disable secure protocols tis1.1 disable Disables the protocol.	clrscrn	Clears the screen.
default secure protocols default top keep alive idle time Defaults the TCP keep alive idle time. default top keep alive interval default top keep alive interval default top keep alive interval default top keep alive probes Exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. son that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text 0xff.="" 255="" <number="" <text="" []="" address="" aes="" assi="" be="" binary="" certificate="" clears="" connect="" connection.="" connections.="" decimal="" decrypt="" default.="" dsa="" encrypt="" establish="" establist="" for="" hex="" host="" initial="" istring="" key.="" mode="" name.="" network="" no="" or="" out="" port="" remote="" removes="" rsa="" selection.="" send="" sent="" sets="" ssh="" string="" text.="" that="" the="" to="" tunnel="" tunneling="" tunneling.="" up="" upon="" use="" used="" user="" will="" within=""> rotocol ssh Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol tep Uses TCP protocol (with AES encryption for connect mode tunneling. Uses TCP protocol (with AES encryption for connect mode tunneling. Protocol tenet Secure protocols sts1.0 disable Secure protocols tts1.0 disable Secure protocols tts1.1 disable Disables the protocol. Examples the protocol. Secure protocols tts1.1 disable Disables the protocol.</text>	credentials <text></text>	
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive interval default tcp keep alive interval default tcp keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary of characterscbinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text dext: = ascii string that will be sent out the network upon connection. no address Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no aes decrypt key no aes encrypt key no aes encrypt key no initial send Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. no initial send Removes the remote port used to establish tunnel connections. no set user timeout Removes the SSH user name. no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunnelingnumber> = number of the port to use. protocol ssh Uses SSH protocol for connect mode tunneling. protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. protocol tcp Uses TCP protocol (with IAC) for connect mode tunneling. secure protocols sti3 on enable secure protocols tis1.0 disable secure protocols tis1.0 enable secure protocols tis1.1 disable Disables the protocol.	default protocol	Restores the default protocol as "TCP".
default tcp keep alive interval default tcp keep alive probes exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect unnel Initial Send text allowing for binary chinary> initial send binary < binary> Sets the host connect tunnel Initial Send text allowing for binary characters. < binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. < text: = ascii string that will be sent out the network upon connection. no address Removes the remote host address used to establish tunneling connections. no aes decrypt key Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string Removes the fost connect tunnel Initial Send string Removes the sSH user name. Removes the SSH user name. Restores the default. Restores the default. Port <number> sets termote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp Uses TCP protocol (with IAE) for connect mode tunneling. Protocol tenet Secure protocols sti3 disable Secure protocols sti3.0 enable Secure protocols tis1.0 disable Secure protocols tis1.1 disable Disables the protocol. Disables the protocol.</number></number>	default secure protocols	Restores the default secure protocol selections.
default tcp keep alive interval default tcp keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <texts <text="" initial="" send="" set=""> sascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the nemote host address used to establish tunneling connections. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the host connect tunnel AES encrypt key. Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tenet Uses Tenet protocol (with IAC) for connect mode tunneling. Secure protocols sts1.0 disable Enables the protocol. Secure protocols sts1.0 disable Enables the protocol. Secure protocols sts1.1 disable Disables the protocol.</number></texts>	default tcp keep alive idle time	Defaults the TCP keep alive idle time.
exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <lext: <="" =="" a="" address="" aed="" aes="" ascii="" be="" certificate="" clears="" connect="" connection.="" connections.="" credentials="" decrypt="" default.="" dsa="" encrypt="" establish="" for="" host="" initial="" key="" key.="" mode="" name.="" network="" no="" out="" port="" remote="" removes="" restores="" rsa="" selection.="" send="" sent="" sets="" ssh="" string="" that="" the="" to="" tunnel="" tunneling="" tunneling.="" upon="" use="" used="" user="" will=""> Port <number> I uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tcp aes Protocol tenet Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP p</number></lext:>	default tcp keep alive interval	
Sets the host connect tunnel Initial Send text allowing for binary characters. binary binary binary binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. texts: a set in the network upon connection. no actions. <a hr<="" td=""><td>default tcp keep alive probes</td><td>Defaults the TCP keep alive probes.</td>	default tcp keep alive probes	Defaults the TCP keep alive probes.
allowing for binary characters. sor hax up to 0xFF. Sets the host connect tunnel Initial Send text. <text: </text: ascii string that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text: </text: ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. no address no aes decrypt key no aes encrypt key no aes encrypt key no aes encrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string no port Removes the remote port used to establish tunnel connections. no ssh username no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunneling. Port <number> Sets the remote port to use for connect mode tunneling. Protocol ssh Protocol ssl Protocol tcp Uses SSH protocol for connect mode tunneling. Protocol tcp aes Protocol tenet Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tenet Uses Telnet protocol. Uses Telnet protocol. Secure protocols stsl.0 disable Enables the protocol. Secure protocols tsl.1.0 disable Disables the protocol.</number>	exit	Exits to the next higher level.
initial send set <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the default. Sets the remote port to use for connect mode tunneling. <number> protocol ssh Uses SSH protocol for connect mode tunneling. protocol ssl Uses SSL protocol for connect mode tunneling. protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. protocol telnet Uses Telnet protocol. secure protocols sl3 enable Enables the protocol. secure protocols tls1.0 disable Disables the protocol. secure protocols tls1.1 disable Disables the protocol.</number></text>	initial send binary send binary orange in the binary >	allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255
no aed decrypt key no aes decrypt key no aes encrypt key no credentials no initial send Removes the host connect tunnel AES decrypt key. no port no port no ssh username no tcp user timeout port <number> protocol ssh protocol tcp protocol tcp protocol telnet protocol telnet secure protocols sls1 on disable secure protocols sls1 on disable secure protocols tls1.0 disable secure protocols tls1.1 disable Disables the protocol. Removes the connect tunnel Initial Send string Removes the nost connect tunnel Initial Send string Removes the PSA/DSA certificate selection. Removes the RSA/DSA certificate selection. Removes the connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the nost connect tunnel Initial Send string Removes the nost connect tunnel Initial Send string Removes the connect tunnel Initial Send string Removes the RSA/DSA certificate selection. Removes the RSA/DSA certificate selection. Removes the Removes the Removes the nost connect tunnel Initial Send string Removes the Removes the Removes the nost connect tunnel Initial Send string Removes the remote port used to establish tunnel Removes the Removes the nost connect mode tunneling. Uses TCP protocol of connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses T</number>	initial send set <text></text>	
no aes encrypt key no credentials Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. no ssh username Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp aes Protocol telnet Secure protocols ssl3 enable Secure protocols tsl1.0 disable Secure protocols tsl1.0 enable Secure protocols tsl1.1 disable Removes the connect tunnel Initial Send string Removes the host connect tunneling Loss TCP protocol for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol</number>	no address	Removes the remote host address used to establish tunneling connections.
no credentials no initial send Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. no ssh username no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh protocol ssl protocol tcp protocol tcp protocol tcp aes protocol telnet secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tsl1.0 disable secure protocols tsl1.0 enable secure protocols tsl1.1 disable Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the host connect tunnel Removes the host connect made. Removes the host connect made. Removes the host connect made. Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connect mode tunneling. Uses SSH protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol.</number></number>	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no initial send Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Enables the protocol. Disables the protocol.</number>	no aes encrypt key	Removes the connect tunnel AES encrypt key.
Removes the remote port used to establish tunnel connections. no ssh username Removes the SSH user name. no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp aes Uses TCP protocol with AES encryption for connect mode tunneling. Protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Disables the protocol. Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Enables the protocol. Disables the protocol.</number>	no credentials	Clears the RSA/DSA certificate selection.
no ssh username no tcp user timeout Port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Protocol ssl Protocol tcp Pro</number></number>	no initial send	Removes the host connect tunnel Initial Send string.
no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh protocol ssl protocol tcp protocol tcp protocol tcp aes Disables the protocol. Secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.1 disable Restores the default. Sets the remote port to use for connect mode tunneling. Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Enables the protocol.</number></number>	no port	·
port <number> Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh Duses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Enables the protocol. Secure protocols tls1.1 disable Disables the protocol.</number></number>	no ssh username	Removes the SSH user name.
protocol ssh protocol ssl protocol ssl protocol tcp protocol tcp aes protocol telnet secure protocols ssl3 enable secure protocols tls1.0 enable secure protocols tls1.0 enable secure protocols tls1.1 disable tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Enables the protocol. Enables the protocol. Enables the protocol. Enables the protocol. Enables the protocol.</number>	no tcp user timeout	
protocol ssl protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol. Disables the protocol. Disables the protocol.	port < <i>number</i> >	
protocol tcp protocol tcp aes Disables the protocols tls1.0 enable protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Enables the protocol. Enables the protocol. Enables the protocol. Disables the protocol.	•	
protocol tcp aes Disables the protocol. Becure protocols tls1.0 enable Becure protocols tls1.1 disable Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Enables the protocol. Disables the protocol. Enables the protocol. Disables the protocol.	•	·
protocol tcp aes mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Enables the protocol.	protocol tcp	•
protocol teinet tunneling. secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Disables the protocol.	protocol tcp aes	mode tunneling.
secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Disables the protocol.	protocol telnet	,
secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Disables the protocol.	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable Enables the protocol. secure protocols tls1.1 disable Disables the protocol.	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable Disables the protocol.	secure protocols tls1.0 disable	Disables the protocol.
·	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 enable Enables the protocol.	·	·
· · ·	secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:6:6) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	, y
host 6 (tunnel-connect-host:5:6) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:4:6) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
cirscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (tunnel-connect-host:3:6) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < <i>number</i> >	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:1:6) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 6 (config-host:6) level commands

clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:16:7) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics

clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 7 (tunnel-connect-host:15:7) level	commands
address < <i>text</i> >	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	[e.,
host 7 (tunnel-connect-host:14:7) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary >	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:13:7) level comma	ands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
	or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:12:7) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:11:7) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary < <i>binary</i> >	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:10:7) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:9:7) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel
	connections.
no ssh username	Removes the SSH user name.
no ssh username no tcp user timeout	Removes the SSH user name. Restores the default.
	Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no tcp user timeout port <number> protocol ssh</number>	Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling.</number>
no tcp user timeout port <number></number>	Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>

protocol tcp aes Uses TCP protocol with AES encryption for connect mode tunnelling.		
secure protocols ssl3 disable secure protocols ssl3 enable secure protocols ssl3 enable secure protocols tsl1.0 disable secure protocols tsl1.0 enable secure protocols tsl1.1 denable secure protocols tsl1.2 disable secure protocols tsl1.2 disable secure protocols tsl1.2 denable secure protocols tsl1.2 denable protocol udp Uses UDP protocol for connect mode tunneling. Show show show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show connection statistics show connection statistics show connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeoutmilliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> sets the immeout for TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timemilliseconds> = timer value, in milliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the immeout for TCP retransmissions. suitidate certificate disable validate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123.3a bc 123.abc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separat</number></number></milliseconds></text></text>	protocol tcp aes	·
secure protocols st3 enable secure protocols st3.0 disable secure protocols tts1.0 enable secure protocols tts1.1 enable secure protocols tts1.1 disable Disables the protocol. secure protocols tts1.1 disable Disables the protocol. secure protocols tts1.1 enable secure protocols tts1.2 disable Disables the protocol. secure protocols tts1.2 enable Disables the protocol. Secure protocols tts1.2 enable Disables the protocol. Secure protocols tts1.2 enable Disables the protocol. Secure protocol tts1.2 enable Disables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling, Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> tcp keep alive interval <milliseconds> sets the timer. <milliseconds> = timer value, in milliseconds. Sets the mumber of TCP keep alive probes. <number> = number of TCP keep alive probes. <number certific<="" certificate="" connecting.="" counted="" for="" of="" server="" solves="" td="" the="" tunnel="" when=""><td>protocol telnet</td><td>, , ,</td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></text>	protocol telnet	, , ,
secure protocols st3 enable secure protocols st3.0 disable secure protocols tts1.0 enable secure protocols tts1.1 enable secure protocols tts1.1 disable Disables the protocol. secure protocols tts1.1 disable Disables the protocol. secure protocols tts1.1 enable secure protocols tts1.2 disable Disables the protocol. secure protocols tts1.2 enable Disables the protocol. Secure protocols tts1.2 enable Disables the protocol. Secure protocols tts1.2 enable Disables the protocol. Secure protocol tts1.2 enable Disables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling, Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> tcp keep alive interval <milliseconds> sets the timer. <milliseconds> = timer value, in milliseconds. Sets the mumber of TCP keep alive probes. <number> = number of TCP keep alive probes. <number certific<="" certificate="" connecting.="" counted="" for="" of="" server="" solves="" td="" the="" tunnel="" when=""><td>secure protocols ssl3 disable</td><td></td></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols ssl3 disable	
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocol secure tonfiguration in permanent memory. secure secur	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocol tldp Uses UDP protocol for connect mode tunneling. Disables the protocol udp Uses UDP protocol with AES encryption for connect mode tunneling. Show Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. < text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. top-keep-alive-probes-time-value, in milliseconds. Sets the immour of TCP keep alive probes. top-keep-alive-probes-time-value, in milliseconds. Sets the immour of TCP keep alive probes. top-keep-alive-probes-time-value, in milliseconds. Sets the immour of TCP keep alive probes. top-keep-alive-probes-time-value, in milliseconds. Sets the timeout for TCP retransmissions. top-keep-alive-probes-time-value, in milliseconds. Sets the connect unnel TCP keep alive probes. top-keep-alive-probes-time-value, in milliseconds. Sets the connect unnel TCP keep alive probes. top-keep-alive-probes-time-v</milliseconds></milliseconds>	secure protocols tls1.0 disable	Disables the protocol.
Secure protocols tls1.1 enable Secure protocols tls1.2 disable Secure protocols tls1.2 disable Secure protocols tls1.2 enable Disables the protocol. Disables the protocol. Disables the protocol. Disables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show history Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> Top keep alive interval <milliseconds> It top keep alive probes <number> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> It top keep alive probes <number> Sets the number of TCP keep alive probes. Sets the number of TCP keep alive probes. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. Walidate certificate disable Sets the timeout value, in milliseconds. Skips verification of the server certificate when connecting. Sets the connect transition of the server certificate when connecting. Sets the connect transition in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC '12 as BC' 12.3a, BC 12.3a, bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC '12 as BC' 12.3a, BC transition of the server certificate enclose the va</number></milliseconds></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.0 enable	Enables the protocol.
Disables the protocol. Secure protocols tls1.2 disable Enables the protocol. Enables the protocol. Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <nilliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <nilliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <nilliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the timeout for TCP retransmissions. <nilliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the timeout for TCP retransmissions. <nilliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the timeout for TCP retransmissions. <nilliseconds> = timer value, in milliseconds> = timer value, in milliseconds. Sets the timeout for TCP retransmissions. <nilliseconds <nilliseconds="timer" =="" for="" i<="" in="" milliseconds="timer" milliseconds.="" retransmissions.="" sets="" tcp="" td="" the="" timeout="" timer="" value,=""><td>secure protocols tls1.1 disable</td><td>Disables the protocol.</td></nilliseconds></nilliseconds></nilliseconds></nilliseconds></nilliseconds></nilliseconds></nilliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	secure protocols tls1.1 disable	Disables the protocol.
Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices.	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes protocol udp aes protocol udp aes show Show the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. sets the mumber of TCP keep alive probes. sets the mount of TCP keep alive probes. sets the mount for TCP retransmissions. sets the mount for TCP retransmissions. sets the mount for TCP retransmissions. sets the timeout for TCP retransmissions. set timeout certificate disable validate certificate disable Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <lext> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bc 12:3a,bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10se the value if it contains spaces.</lext></milliseconds></milliseconds></text></text>	secure protocols tls1.2 disable	Disables the protocol.
Uses UDP protocol with AES encryption for connect mode tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = temper value, in milliseconds. Explayed and the set of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timer value, in milliseconds> = timer value, in milliseconds = timer value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timer value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Validate certificate enable Validate certificate enable Validate certificate enable Sets the current configuration in permanent memory. Nost 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC" 14 3A BC</text></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds> top keep alive interval <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host 8.7) level commands address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces.</text></text></milliseconds></number></number></milliseconds></milliseconds></milliseconds></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout, <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Validate certificate disable Skips verification of the server certificate when connecting. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. Most 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections the value if it contains spaces.</text></milliseconds></number></milliseconds></milliseconds></milliseconds></milliseconds></text>	protocol udp aes	
show statistics show connection statistics sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> to keep alive interval <milliseconds> to keep alive probes <number> to keep alive probes <number> to keep alive probes <number> to user timeout <milliseconds> to user timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> timeout value, in milliseconds. Sets the timeout value, in milliseconds. Sets the current configuration of the server certificate when connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands address <text> to user timeout value, in milliseconds to user timeout value, in milliseconds. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,BC 12.3a,BC 12.3a,BC 12.3a,BC 12.3a,BC 12.3a,BC 12.3a,BC 12.3a,BC 12.3a,B</text></text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Set she TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds. <number="" =="" alive="" in="" keep="" milliseconds.="" probes="" tcp="" timer="" value,=""> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Sets the current configuration in permanent memory. host 7 (tunnel-connect-host:3:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></number></number></number></milliseconds.></milliseconds></text>	show history	
tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write</milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></text>	show statistics	show connection statistics
keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <lext> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</lext></milliseconds></milliseconds></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
and sets the timer. <milliseconds> = timer value, in milliseconds. top keep alive probes <number> top keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2;3A,BC 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></milliseconds></number></number></number></number></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
conumber> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout for TCP retransmissions. smilliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to Sets the connect tunnel AES decrypt key with up to</text></milliseconds>	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
cp user timeout <milliseconds> smilliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. write Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to Sets the connect tunnel AES decrypt key with up to</text></milliseconds>	tcp keep alive probes <number></number>	
validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp user timeout <milliseconds></milliseconds>	
connecting. Stores the current configuration in permanent memory. host 7 (tunnel-connect-host:8:7) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 sets the conne</text>	validate certificate disable	
memory. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	validate certificate enable	· •
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	write	
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 7 (tunnel-connect-host:8:7) level com	
16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <i><hexadecimal></hexadecimal></i>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	aes decrypt key text <text></text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
	Uses Telnet protocol (with IAC) for connect mode
protocol telnet	tunneling.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tis1.0 enable	Enables the protocol.
secure protocols tIs1.1 disable	Disables the protocol.
secure protocols tis1.1 enable	Enables the protocol.
secure protocols tIs1.2 disable	Disables the protocol.
secure protocols tis1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol dup	Uses UDP protocol with AES encryption for connect
protocol udp aes	mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:7:7) level command:	5
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:6:7) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a:bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a:bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single.</text>		
connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. The contains spaces are not provided by a single character. The contains spaces are not provided by a single character. The contains spaces are not provided by a single character. The contains spaces are not provided by a single character. The contains space are not provided by a single character. The contains space are not provided by a single character. The contains space are not provided by a single character. The contains space are not provided by a single character are not provided by a single character. The contains space are not provided by a single character are not provided by a single character. The contains space are not provided by a single character are not provided by a single character. The contains space are not provided by a single character are not provided by a single character. The contains space are not provided by a single character are not provided by a sing</text>	host 7 (tunnel-connect-host:5:7) level commands	
16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single single.	address <text></text>	connections with. <text> = IP address or host name</text>
es decrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single.</text>	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
tes encrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single.</hexadecimal>	aes decrypt key text < text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
16 bytes. Each byte is represented by a single	aes encrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
es encrypt key text < text> character. Note that quotes must enclose the value if it contains spaces.	aes encrypt key text < text>	16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value
uto show statistics show connection statistics	auto show statistics	show connection statistics
Irscrn Clears the screen.	clrscrn	Clears the screen.
redentials <text> Selects the RSA/DSA certificates by name for the SSL client.</text>	credentials <text></text>	•
efault protocol Restores the default protocol as "TCP".	default protocol	Restores the default protocol as "TCP".
efault secure protocols Restores the default secure protocol selections.	default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:4:7) level command	ls
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
credentials <text> default protocol default secure protocols default tcp keep alive idle time default tcp keep alive interval default tcp keep alive probes</text>	Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol as "TCP". Restores the default secure protocol selections. Defaults the TCP keep alive idle time. Restores the default 45 second connect mode TC keep alive timeout. Defaults the TCP keep alive probes.

	Sets the host connect tunnel Initial Send text
initial send binary sinary>	allowing for binary characters. send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (tunnel-connect-host:3:7) level comma	nds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:1:7) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
	Removes the remote port used to establish tunnel
no port	connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 7 (config-host:7) level commands

clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

host 8 (tunnel-connect-host:16:8) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics

clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	memory.
host 8 (tunnel-connect-host:15:8) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 8 (tunnel-connect-host:14:8) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	•
host 8 (tunnel-connect-host:13:8) level of	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
	or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 8 (tunnel-connect-host:12:8) level co	mmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:11:8) level (commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 8 (tunnel-connect-host:10:8) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no initial send no port	Removes the host connect tunnel Initial Send string. Removes the remote port used to establish tunnel connections.
	Removes the remote port used to establish tunnel

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:9:8) level com	mands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

	Uses TCP protocol with AES encryption for connect
protocol tcp aes	mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
	Sets the SSH user name for use when establishing
ssh username <text></text>	tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:8:8) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single

	character. Note that quotes must enclose the value
	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tis1.0 enable	Enables the protocol.
secure protocols tIs1.1 disable	Disables the protocol.
secure protocols tis1.1 enable	Enables the protocol.
secure protocols tIs1.2 disable	Disables the protocol.
secure protocols tis1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol dup	Uses UDP protocol with AES encryption for connect
protocol udp aes	mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:7:8) level command:	5
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

aes encrypt key text <text> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics show connection statistics cIrscrn Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default top keep alive idle time Defaults the TCP keep alive idle time. default top keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default top keep alive probes Defaults the TCP keep alive probes. exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. </text>		12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must
aes encrypt key text < lext> 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics show connection statistics clears the screen. Clears the screen. Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default ttop keep alive idle time Defaults the TCP keep alive idle time. default top keep alive interval Restores the default 45 second connect mode TCP keep alive probes Defaults the TCP keep alive probes. Exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. cbinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. < exchange in the network upon connection. no address initial send set no address no aes decrypt key no aes encrypt key no aes encrypt key no aes encrypt key no aes encrypt key no eredentials no port connections. Removes the connect tunnel Initial Send text. < exchange in the network upon connection. Removes the connect tunnel AES decrypt key. Removes the remote port used to establish tunnel connections. Removes the host connect tunnel Initial Send string Removes the SBH user name. Restores the default. Sets the remote port used to establish tunnel connections. Removes the SBH user name. Restores the default. Sets the remote port to use for connect mode tunneling. Uses SSL protocol for connect		·
Clears the screen. Selects the RSA/DSA certificates by name for the SSL client. Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol as "TCP". default secure protocols Restores the default secure protocol selections. default tcp keep alive idle time Defaults the TCP keep alive idle time. Restores the default 45 second connect mode TCP keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default tcp keep alive interval Restores the default 45 second connect mode TCP keep alive timeout. default tcp keep alive probes Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters, chinary> string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text: <number="" address="" aes="" ascii="" be="" certificate="" clears="" connect="" connection.="" connections.="" decrypt="" default.="" dort="" dsa="" encrypt="" establish="" host="" initial="" key.="" nest="" network="" out="" port="" remote="" removes="" restores="" rsa="" selection.="" send="" sent="" string="" that="" the="" to="" tunnel="" tunneling="" upon="" used="" will=""> Removes the remote port to use for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp Uses SSL protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Protocol telnet SECURD Protocol (with IAC) for connect mode tunneling. Disables the protocol. Disables the protocol. Disables the protocol.</text:>	aes encrypt key text <text></text>	character. Note that quotes must enclose the value
Selects the RSA/DSA certificates by name for the SSL client. Restores the default protocol Restores the default protocol as "TCP". Restores the default secure protocol selections. Restores the default secure protocol. Restores the default. Res	auto show statistics	show connection statistics
default protocol default secure protocols default secure protocols default secure protocols default to keep alive idle time default top keep alive idle time default top keep alive interval default top keep alive interval default top keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characterschinary> = string in initial send binary -binary> binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text, -text: = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no ase decrypt key no ase encrypt key no ase encrypt key no ase encrypt key no credentials Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling, -rumber> protocol ssh Uses SSL protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tepnet Uses TCP protocol (with IAC) for connect mode tunneling. Protocol telnet Secure protocols tis1.0 disable Secure protocols Secure protocols tis1.1 disable Disables the protocol.	clrscrn	Clears the screen.
default secure protocols default top keep alive idle time Defaults the TCP keep alive idle time. default top keep alive interval default top keep alive interval default top keep alive interval default top keep alive probes Exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. son that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text 0xff.="" 255="" <number="" <text="" []="" address="" aes="" assi="" be="" binary="" certificate="" clears="" connect="" connection.="" connections.="" decimal="" decrypt="" default.="" dsa="" encrypt="" establish="" establist="" for="" hex="" host="" initial="" istring="" key.="" mode="" name.="" network="" no="" or="" out="" port="" remote="" removes="" rsa="" selection.="" send="" sent="" sets="" ssh="" string="" text.="" that="" the="" to="" tunnel="" tunneling="" tunneling.="" up="" upon="" use="" used="" user="" will="" within=""> rotocol ssh Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Protocol tep Uses TCP protocol (with AES encryption for connect mode tunneling. Uses TCP protocol (with AES encryption for connect mode tunneling. Protocol tenet Secure protocols sts1.0 disable Secure protocols tts1.0 disable Secure protocols tts1.1 disable Disables the protocol. Examples the protocol. Secure protocols tts1.1 disable Disables the protocol.</text>	credentials <text></text>	
default tcp keep alive idle time default tcp keep alive interval default tcp keep alive interval default tcp keep alive interval default tcp keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary of characterscbinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text dext: = ascii string that will be sent out the network upon connection. no address Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. no aes decrypt key no aes encrypt key no aes encrypt key no initial send Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. no initial send Removes the remote port used to establish tunnel connections. no set user timeout Removes the SSH user name. no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunnelingnumber> = number of the port to use. protocol ssh Uses SSH protocol for connect mode tunneling. protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. protocol tcp Uses TCP protocol (with IAC) for connect mode tunneling. secure protocols sti3 on enable secure protocols tis1.0 disable secure protocols tis1.0 enable secure protocols tis1.1 disable Disables the protocol.	default protocol	Restores the default protocol as "TCP".
default tcp keep alive interval default tcp keep alive probes exit Defaults the TCP keep alive probes. Exits to the next higher level. Sets the host connect unnel Initial Send text allowing for binary chinary> initial send binary < binary> Sets the host connect tunnel Initial Send text allowing for binary characters. < binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. < text: = ascii string that will be sent out the network upon connection. no address Removes the remote host address used to establish tunneling connections. no aes decrypt key Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string Removes the fost connect tunnel Initial Send string Removes the sSH user name. Removes the SSH user name. Restores the default. Restores the default. Port <number> Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Protocol tcp aes Protocol tenet Uses TCP protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 enable Enables the protocol. Enables the protocol. Enables the protocol. Enables the protocol.</number></number>	default secure protocols	Restores the default secure protocol selections.
default tcp keep alive interval default tcp keep alive probes exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <texts <text="" initial="" send="" set=""> sascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the nemote host address used to establish tunneling connections. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the host connect tunnel AES encrypt key. Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tenet Uses Tenet protocol (with IAC) for connect mode tunneling. Secure protocols sts1.0 disable Enables the protocol. Secure protocols sts1.0 disable Enables the protocol. Secure protocols sts1.1 disable Disables the protocol.</number></texts>	default tcp keep alive idle time	Defaults the TCP keep alive idle time.
exit Exits to the next higher level. Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <lext: <="" =="" a="" address="" aed="" aes="" ascii="" be="" certificate="" clears="" connect="" connection.="" connections.="" credentials="" decrypt="" default.="" dsa="" encrypt="" establish="" for="" host="" initial="" key="" key.="" mode="" name.="" network="" no="" out="" port="" remote="" removes="" restores="" rsa="" selection.="" send="" sent="" sets="" ssh="" string="" that="" the="" to="" tunnel="" tunneling="" tunneling.="" upon="" use="" used="" user="" will=""> Port <number> I uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSL protocol for connect mode tunneling. Protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tcp aes Protocol tenet Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP p</number></lext:>	default tcp keep alive interval	
Sets the host connect tunnel Initial Send text allowing for binary characters. binary binary binary binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. texts: a set in the network upon connection. no actions. <a hr<="" td=""><td>default tcp keep alive probes</td><td>Defaults the TCP keep alive probes.</td>	default tcp keep alive probes	Defaults the TCP keep alive probes.
allowing for binary characters. sor hax up to 0xFF. Sets the host connect tunnel Initial Send text. <text: </text: ascii string that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF. Sets the host connect tunnel Initial Send text. <text: </text: ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. no address no aes decrypt key no aes encrypt key no aes encrypt key no aes encrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string no port Removes the remote port used to establish tunnel connections. no ssh username no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunneling. Port <number> Sets the remote port to use for connect mode tunneling. Protocol ssh Protocol ssl Protocol tcp Uses SSH protocol for connect mode tunneling. Protocol tcp aes Protocol tenet Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Protocol tenet Uses Telnet protocol. Uses Telnet protocol. Secure protocols stsl.0 disable Enables the protocol. Secure protocols tsl.1.0 disable Disables the protocol.</number>	exit	Exits to the next higher level.
initial send set <text> = ascii string that will be sent out the network upon connection. Removes the remote host address used to establish tunneling connections. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key. Removes the connect tunnel AES encrypt key. Removes the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. Removes the remote port used to establish tunnel connections. Removes the default. Sets the remote port to use for connect mode tunneling. <number> protocol ssh Uses SSH protocol for connect mode tunneling. protocol ssl Uses SSL protocol for connect mode tunneling. protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. protocol telnet Uses Telnet protocol. secure protocols sl3 enable Enables the protocol. secure protocols tls1.0 disable Disables the protocol. secure protocols tls1.1 disable Disables the protocol.</number></text>	initial send binary send binary orange in the binary >	allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255
no aed decrypt key no aes decrypt key no aes encrypt key no credentials no initial send Removes the host connect tunnel AES decrypt key. no port no port no ssh username no tcp user timeout port <number> protocol ssh protocol tcp protocol tcp protocol telnet protocol telnet secure protocols sls1 on disable secure protocols sls1 on disable secure protocols tls1.0 disable secure protocols tls1.1 disable Disables the protocol. Removes the connect tunnel Initial Send string Removes the nost connect tunnel Initial Send string Removes the PSA/DSA certificate selection. Removes the RSA/DSA certificate selection. Removes the connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the nost connect tunnel Initial Send string Removes the nost connect mode tunneling. Uses SSH user name. Removes the remote port to use for connect mode tunneling. Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Disables the protocol.</number>	initial send set <text></text>	
no aes encrypt key no credentials Clears the RSA/DSA certificate selection. no initial send Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. no ssh username Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp aes Protocol telnet Secure protocols ssl3 enable Secure protocols tsl1.0 disable Secure protocols tsl1.0 enable Secure protocols tsl1.1 disable Removes the connect tunnel Initial Send string Removes the host connect tunneling Loss TCP protocol for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses TCP protocol</number>	no address	Removes the remote host address used to establish tunneling connections.
no credentials no initial send Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. no ssh username no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh protocol ssl protocol tcp protocol tcp protocol tcp aes protocol telnet secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tsl1.0 disable secure protocols tsl1.0 enable secure protocols tsl1.1 disable Clears the RSA/DSA certificate selection. Removes the host connect tunnel Initial Send string Removes the host connect tunnel Initial Send string Removes the host connect tunnel Removes the host connect made. Removes the host connect made. Removes the host connect made. Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connect mode tunneling. Uses SSH protocol (with IAC) for connect mode tunneling. Uses TCP protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol.</number></number>	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no initial send Removes the host connect tunnel Initial Send string Removes the remote port used to establish tunnel connections. Removes the SSH user name. Removes the default. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Enables the protocol. Disables the protocol.</number>	no aes encrypt key	Removes the connect tunnel AES encrypt key.
Removes the remote port used to establish tunnel connections. no ssh username Removes the SSH user name. no tcp user timeout Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol tcp Uses TCP protocol for connect mode tunneling. Protocol tcp aes Uses TCP protocol with AES encryption for connect mode tunneling. Protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Disables the protocol. Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Enables the protocol. Disables the protocol.</number>	no credentials	Clears the RSA/DSA certificate selection.
no ssh username no tcp user timeout Port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Protocol ssh Protocol ssl Protocol tcp Pro</number></number>	no initial send	Removes the host connect tunnel Initial Send string.
no tcp user timeout port <number> Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh protocol ssl protocol tcp protocol tcp protocol tcp aes Disables the protocol. Secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.1 disable Restores the default. Sets the remote port to use for connect mode tunneling. Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Enables the protocol.</number></number>	no port	·
port <number> Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. protocol ssh Duses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Enables the protocol. Secure protocols tls1.1 disable Disables the protocol.</number></number>	no ssh username	Removes the SSH user name.
protocol ssh protocol ssl protocol ssl protocol tcp protocol tcp aes protocol telnet secure protocols ssl3 enable secure protocols tls1.0 enable secure protocols tls1.0 enable secure protocols tls1.1 disable tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Enables the protocol. Enables the protocol.</number>	no tcp user timeout	
protocol ssl protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Secure protocols ssl3 disable Secure protocols ssl3 enable Secure protocols tls1.0 disable Disables the protocol. Secure protocols tls1.0 enable Secure protocols tls1.1 disable Disables the protocol. Disables the protocol. Disables the protocol.	port < <i>number</i> >	
protocol tcp protocol tcp aes Disables the protocols tls1.0 enable protocol tcp Uses TCP protocol for connect mode tunneling. Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Enables the protocol. Enables the protocol. Enables the protocol. Disables the protocol.	•	
protocol tcp aes Disables the protocol. Becure protocols tls1.0 enable Becure protocols tls1.1 disable Uses TCP protocol with AES encryption for connect mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. Disables the protocol. Enables the protocol. Enables the protocol. Disables the protocol. Enables the protocol. Disables the protocol.	•	·
protocol tcp aes mode tunneling. Uses Telnet protocol (with IAC) for connect mode tunneling. secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Enables the protocol.	protocol tcp	•
protocol teinet tunneling. secure protocols ssl3 disable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Disables the protocol.	protocol tcp aes	mode tunneling.
secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Enables the protocol. Disables the protocol.	protocol telnet	,
secure protocols tls1.0 disable secure protocols tls1.0 enable secure protocols tls1.1 disable Disables the protocol. Disables the protocol.	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable Enables the protocol. secure protocols tls1.1 disable Disables the protocol.	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable Disables the protocol.	secure protocols tls1.0 disable	Disables the protocol.
·	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 enable Enables the protocol.	·	·
· · ·	secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 8 (tunnel-connect-host:6:8) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	1
host 8 (tunnel-connect-host:5:8) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	momory.
host 8 (tunnel-connect-host:3:8) level commands	S
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:1:8) level co	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel
	connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 8 (config-host:8) level commands

clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

host 9 (tunnel-connect-host:16:9) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics

clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 9 (tunnel-connect-host:15:9) level of	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,e.,,
host 9 (tunnel-connect-host:14:9) level of	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	<u> </u>
host 9 (tunnel-connect-host:13:9) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
	or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

mands
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:11:9) level	commands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < <i>text</i> >	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
•	Sets the remote port to use for connect mode
port <number></number>	tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 9 (tunnel-connect-host:10:9) level commands

address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.

port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:9:9) level command	ds
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated

	by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel
	connections.
no ssh username	Removes the SSH user name.
no ssh username no tcp user timeout	Removes the SSH user name. Restores the default.
	Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no tcp user timeout port <number> protocol ssh</number>	Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use. Uses SSH protocol for connect mode tunneling.</number>
no tcp user timeout port <number></number>	Removes the SSH user name. Restores the default. Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>

milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting.</milliseconds></number></number></number></milliseconds>		
secure protocols ssl3 disable secure protocols ssl3 enable secure protocols ssl3 enable secure protocols tls1.0 disable secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 enable Enables the protocol. Secure protocol tls1.2 enable Enables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Show stee current configuration. Show show history Shows the current configuration. Show statistics Show connection statistics Sets the SFA user name for use when establishing tunneling connections with other devices, <text> = SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> connecting. Sets the number of TCP keep alive probes. Sets the timer. <milliseconds> = timer value, in milliseconds. Sets the timeout for TCP keep alive probes. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP keep alive probes. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <mi><milliseconds> = timeout value, in milliseconds. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex di</milliseconds></mi></milliseconds></mi></milliseconds></mi></milliseconds></mi></milliseconds></mi></milliseconds></milliseconds></milliseconds></text></text>	protocol tcp aes	
secure protocols ss13 enable Enables the protocol. secure protocols tls1.0 disable secure protocols tls1.1 denable Secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.1 disable Secure protocols tls1.2 disable Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Enables the protocol. Secure protocol tls1.2 enable Enables the protocol. Secure protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Shows Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices, <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Top keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. Skips verification of the server certificate when connecting. Skips the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represen</number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text>	protocol telnet	
secure protocols tls1.0 disable secure protocols tls1.1 onable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 enable Enables the protocol. Secure protocols tls1.2 enable Disables the protocol. Secure protocols tls1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show the current configuration. Displays the last 20 commands entered during the current Cul session. Show show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing unneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive itimeout. <milliseconds> = timer value, in milliseconds> tcp keep alive interval <milliseconds> Sets the TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. cpuser timeout <milliseconds> Sets the number of TCP keep alive probes. squildate certificate disable validate certificate enable Sets the number of TCP keep alive probes. Sets the number of TCP keep alive probes. Sets the timeout for TCP retransmissions. **milliseconds> = timeout value, in milliseconds. Sets the current configuration in permanent memory. **Total Current Configuration in permanent memory. **Sets the current configuration in permanent memory. **Sets the current tonel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC **123ABC** 123ABC** 123A</milliseconds></milliseconds></milliseconds></milliseconds></text>	secure protocols ssl3 disable	Disables the protocol.
secure protocols tls1.0 enable secure protocols tls1.1 disable secure protocols tls1.1 enable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable secure protocols tls1.2 enable secure protocols tls1.2 enable protocol udp Disables the protocol. secure protocol tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Show such a current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> ctp keep alive probes <number> sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <number (tunnel-connect-host.8:9)="" 9="" <number="" <text="" alive="" and="" certificate="" commands="" configuration="" connect="" connecting.="" connections="" current="" enable="" establish="" for="" host="" in="" inst="" keep="" level="" memory.="" number="" of="" permanent="" probes.="" remote="" requires="" retransmissions.="" server="" sets="" stores="" tcp="" the="" timeout="" to="" tunneling="" tunuel="" validate="" verification="" when="" with.=""> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC" 12 3A BC "12 3A BC" 12 3A BC "12 3A BC "12 3A BC "12 3A BC "12</number></number></number></number></milliseconds></number></milliseconds></milliseconds></text>	secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.1 disable secure protocols tls1.2 enable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp protocol udp protocol udp protocol udp aes show Shows tls2 urrent configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics show connection statistics show connection swith other devices. <text> = SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> = number of TCP keep alive probes. <number> number of TC</number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></number></milliseconds></milliseconds></text></text>	secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.1 enable secure protocols tls1.2 disable secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp protocol udp protocol udp protocol udp show show show show istory show statistics show statistics show statistics show some current configuration. Displays the last 20 commands entered during the current CLI session. show show statistics show connection statistics show connection statistics show connection statistics show connection statistics show ename <text> Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> cp user timeout <milliseconds> sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123 AB C" 12.3A, BC 12.3a, bc 12:3a, bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "123 AB C" 12.3A, BC 12.3a, bc 12.3a,</text></milliseconds></milliseconds></number></number></milliseconds></number></milliseconds></milliseconds></text></text>	secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.2 disable secure protocols tls1.2 enable protocol udp Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics show connection statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. ctext> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> top keep alive interval <milliseconds> top keep alive probes <number> top keep alive probes <number> top user timeout <milliseconds> sets the timeout for TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. shilliseconds> = timeout value, in milliseconds skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC '12 3A BC'' 12.3A,BC 12.3a,bc 12:3a,bc Value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</number></number></number></number></number></number></number></milliseconds></number></number></milliseconds></milliseconds>	secure protocols tls1.1 disable	Disables the protocol.
secure protocol stls1.2 enable Enables the protocol. Uses UDP protocol for connect mode tunneling. Uses UDP protocol for connect mode tunneling. Uses UDP protocol with AES encryption for connect mode tunneling. Show show with AES encryption for connect mode tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP retransisions. validate certificate disable validate certificate disable validate certificate enable Requires verification of the server certificate when connecting. Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 connections. Sets the connect tunnel AES decrypt key with up to 10 connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12.3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 15 bytes. Each byt</text></text></number></number></number></number></milliseconds></milliseconds></text>	secure protocols tls1.1 enable	Enables the protocol.
protocol udp aes protocol udp aes show Show be current configuration. Displays the last 20 commands entered during the current CLI session. show statistics show statistics show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive interval <milliseconds> tcp keep alive interval <milliseconds> tcp keep alive probes <number> current CLI session. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the mount for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the current for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Skips verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 10 systems of tunnel AES decrypt key with up to 10 systems of tunnel AES decrypt key with up to 10 systems of tunnel AES decrypt key with up to 10 sy</text></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></number></milliseconds></milliseconds></text>	secure protocols tls1.2 disable	Disables the protocol.
protocol udp aes show Show tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Sets the current configuration in permanent memory. Inost 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with . address <text> Sets the remote host to establish tunneling connections with . address <text> Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC"</text></text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	secure protocols tls1.2 enable	Enables the protocol.
protocol udp aes show Show tunneling. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. <milliseconds> = timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Sets the imeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Sets the current configuration in permanent memory. Inost 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with . address <text> Sets the remote host to establish tunneling connections with . address <text> Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12 3A BC"</text></text></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></number></number></milliseconds></milliseconds></text>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history Displays the last 20 commands entered during the current CLI session. show statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive itimeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive interval <milliseconds> tcp keep alive probes <number> Sets the number of TCP keep alive probes. cumber> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. cmilliseconds> = timeout value, in milliseconds. Sets the timeout for TCP retransmissions. cmilliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. Inost 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 102.3a.bc Note that quotes must enclose the value if it contains spaces.</text></number></milliseconds></milliseconds></milliseconds></text>	protocol udp aes	Uses UDP protocol with AES encryption for connect
show statistics show connection statistics Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive imeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Write Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. **Note of tunnel-connect-host:8:9} level commands** Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces.</text></milliseconds></number></number></milliseconds></milliseconds></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive idle time <milliseconds></milliseconds></text>	show history	
tunneling connections with other devices. <text> = SSH user name. Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds. tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 200 connections with contains spaces. Sets the connect tunnel AES decrypt key with up to 200 connections with contains spaces.</text></milliseconds></number></number></number></milliseconds></milliseconds></text>	show statistics	show connection statistics
keep alive idle time <milliseconds> keep alive timeout. <milliseconds> = timer value, in milliseconds. Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds> tcp keep alive probes <number> tcp keep alive probes <number> Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. <number> = number of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Validate certificate enable validate certificate enable validate certificate enable Stores the current configuration in permanent memory. **Note of the server certificate when connecting.** Stores the current configuration in permanent memory. **Note of the server certificate when connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 2 optional punctuation: 123ABC Note that quotes must enclose the value if it contains spaces.</text></milliseconds></number></number></number></number></milliseconds></milliseconds></milliseconds>	ssh username <text></text>	tunneling connections with other devices. <text> =</text>
tcp keep alive interval <milliseconds> and sets the timer. <milliseconds> = timer value, in milliseconds. Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes. tcp user timeout <milliseconds> Sets the timeout of TCP keep alive probes. Sets the timeout of TCP keep alive probes. Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds. Skips verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 9 (tunnel-connect-host:8;9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 200 decrypt key uton up to 200 dec</text></milliseconds></milliseconds></number></milliseconds></milliseconds>	tcp keep alive idle time <milliseconds></milliseconds>	keep alive timeout. <milliseconds> = timer value, in</milliseconds>
cnumber number	tcp keep alive interval <milliseconds></milliseconds>	and sets the timer. <milliseconds> = timer value, in</milliseconds>
validate certificate disable validate certificate disable validate certificate enable validate certificate enable Requires verification of the server certificate when connecting. Requires verification of the server certificate when connecting. Write Stores the current configuration in permanent memory. host 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to Sets the connect tunnel AES decrypt key with up to</text>	tcp keep alive probes <number></number>	
validate certificate enable Requires verification of the server certificate when connecting. Stores the current configuration in permanent memory. host 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	tcp user timeout <milliseconds></milliseconds>	
connecting. Stores the current configuration in permanent memory. host 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to 50 connections. Sets the connect tunnel AES decrypt key with up to 50 connections.</text>	validate certificate disable	·
memory. host 9 (tunnel-connect-host:8:9) level commands Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text>	validate certificate enable	
address <text> Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	write	·
address <text> connections with. <text> = IP address or host name of the remote host. Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</text></text>	host 9 (tunnel-connect-host:8:9) level com	mands
aes decrypt key <hexadecimal> 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Sets the connect tunnel AES decrypt key with up to</hexadecimal>	address <text></text>	connections with. <text> = IP address or host name</text>
	aes decrypt key <hexadecimal></hexadecimal>	16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
	aes decrypt key text < text>	

	character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.

secure protocols ssl3 enable	Enables the protocol.
secure protocols sist enable	Disables the protocol.
secure protocols tis1.0 disable	Enables the protocol.
secure protocols tis1.0 enable	Disables the protocol.
secure protocols tis1.1 disable	Enables the protocol.
secure protocols tis1.1 enable	Disables the protocol.
secure protocols tis1.2 disable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocor dup	Uses UDP protocol with AES encryption for connect
protocol udp aes	mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:7:9) level command	S
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC"

	12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.

secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 9 (tunnel-connect-host:6:9) level command	S
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes < number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 9 (tunnel-connect-host:5:9) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.

default tcp keep alive idle time	Defaults the TCP keep alive idle time.
	Restores the default 45 second connect mode TCP
default tcp keep alive interval	keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. <binary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.</binary>
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>

tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <pre><number> = number of TCP keep alive probes.</number></pre>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

S
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.

initial send binary sinary>	Sets the host connect tunnel Initial Send text allowing for binary characters. binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>

tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

	,
host 9 (tunnel-connect-host:3:9) level con	nmands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text < text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. send text allowing for binary characters. binary format that will be sent out the network upon

	connection. Within [] use binary decimal up to 255
	or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
	Uses TCP protocol with AES encryption for connect
protocol tcp aes	mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>

tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

ds
Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
show connection statistics
Clears the screen.
Selects the RSA/DSA certificates by name for the SSL client.
Restores the default protocol as "TCP".
Restores the default secure protocol selections.
Defaults the TCP keep alive idle time.
Restores the default 45 second connect mode TCP keep alive timeout.
Defaults the TCP keep alive probes.
Exits to the next higher level.
Sets the host connect tunnel Initial Send text allowing for binary characters. sinary = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:1:9) level c	ommands
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <text></text>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default secure protocols	Restores the default secure protocol selections.
default tcp keep alive idle time	Defaults the TCP keep alive idle time.
default tcp keep alive interval	Restores the default 45 second connect mode TCP keep alive timeout.
default tcp keep alive probes	Defaults the TCP keep alive probes.
exit	Exits to the next higher level.
initial send binary <binary></binary>	Sets the host connect tunnel Initial Send text allowing for binary characters. sinary> = string in binary format that will be sent out the network upon connection. Within [] use binary decimal up to 255 or hex up to 0xFF.
initial send set <text></text>	Sets the host connect tunnel Initial Send text. <text> = ascii string that will be sent out the network upon connection.</text>
no address	Removes the remote host address used to establish tunneling connections.
	D 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
no aes decrypt key no aes encrypt key	Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key.

no credentials	Clears the RSA/DSA certificate selection.
no initial send	Removes the host connect tunnel Initial Send string.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp user timeout	Restores the default.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
secure protocols tls1.2 disable	Disables the protocol.
secure protocols tls1.2 enable	Enables the protocol.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive idle time <milliseconds></milliseconds>	Sets the TCP keep alive idle time. This is the initial keep alive timeout. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive interval <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
tcp keep alive probes <number></number>	Sets the number of TCP keep alive probes. <number> = number of TCP keep alive probes.</number>
tcp user timeout <milliseconds></milliseconds>	Sets the timeout for TCP retransmissions. <milliseconds> = timeout value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.

host 9 (config-host:9) level commands

clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <number></number>	Change to config host level
name <text></text>	Sets the name of the host. <text> = name of the host.</text>
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <text></text>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.</text>
remote port <number></number>	Sets the remote port used to connect to the host. <number> = port to be used.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <text></text>	Sets the username for logging into the host via SSH. <text> = username.</text>
write	Stores the current configuration in permanent memory.

http (config-http) level commands	
auth < <i>uri</i> >	Creates a new HTTP server authentication directive. <uri> = URI of the server.</uri>
auth type <uri> digest</uri>	Sets an HTTP server authentication directive to the Digest Access Authentication scheme. <uri> = URI of the server.</uri>
auth type <uri> none</uri>	Sets the authentication type for an HTTP server authentication directive to none. <uri> = URI of the server.</uri>
auth type <uri> ssl</uri>	Sets the authentication type for an HTTP server authentication directive to SSL. <uri> = URI of the server.</uri>
auth type <uri> ssl-basic</uri>	Sets the authentication type for an HTTP server authentication directive to SSL-Basic. <uri> = URI of the server.</uri>
auth type <uri>> ssl-digest</uri>	Sets the authentication type for an HTTP server authentication directive to SSL-Digest. <uri> = URI of the server.</uri>
authentication timeout <minutes></minutes>	For any Digest AuthType, sets the timeout for authentication. <minutes> = authentication timeout value.</minutes>
clear counters	Sets the HTTP counters to zero.
clear log	Clears the HTTP server log.
clrscrn	Clears the screen.

default authentication timeout	Resets the authentication timeout to its default value.
default log format	Restores the HTTP Server log format string to its default value.
default max bytes	Resets the maximum bytes to its default value.
default max log entries	Restores the default maximum number of HTTP Server log entries.
default max timeout	Resets the timeout to its default value.
default port	Resets the HTTP Server port to its default value.
default secure port	Resets the HTTP Server SSL port to its default value.
delete auth <uri></uri>	Deletes an existing HTTP Server authentication directive. <uri> = URI of the server.</uri>
exit	Returns to the config level.
log format <text></text>	Sets the log format string for the HTTP server, using the following directives: %a remote ip address (could be a proxy) %b bytes sent excluding headers %B bytes sent excluding headers (0 = '-') %h remote host (same as %a) %{h}i header contents from request (h = header string) %m request method %p ephemeral local port value used for request %q query string (prepend with '?' or empty '-') %t timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t') %u remote user (could be bogus for 401 status) %U URL path info %r first line of request (same as '%m %U%q <version>') %s return status</version>
logging state disable	Disables HTTP server logging.
logging state enable	Enables HTTP server logging.
max bytes < <i>number</i> >	Sets the maximum number of bytes the HTTP server accepts when receiving a request.
max log entries < number>	Sets the maximum number of HTTP server log entries. <number> = maximum number of HTTP server log entries.</number>
max timeout <seconds></seconds>	Sets the maximum time the HTTP server waits when receiving a request. <seconds> = maximum timeout value.</seconds>
no clear counters	Restores the HTTP counters to the aggregate values.
no port	Disables the HTTP Server port.
no secure credentials	Clears the RSA/DSA certificate selection.
no secure port	Disables the HTTP Server SSL port.
port <number></number>	Sets the port number the HTTP server will use. <pre><number> = port number.</number></pre>
secure credentials <text></text>	Selects the RSA/DSA certificates by name for the HTTP server.
secure port <number></number>	Sets the port number the HTTP server will use over SSL. <number> = port number.</number>
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
ocoure protocola aala eriable	Enables the protestin

secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
show	Displays the current configuration.
show auth	Displays the HTTP server authentication settings.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the HTTP server log.
show statistics	Displays the HTTP statistics.
state disable	Disables the HTTP server.
state enable	Enables the HTTP server.
write	Stores the current configuration in permanent memory.

http post (config-action-http_post:on scheduled	reboot) level commands
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the HTTP Post reminder interval. HTTP Post is sent once only.
reminder interval <minutes></minutes>	Sets the HTTP Post reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

http post (config-action-http_post:eth2 link state change) level commands	
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the HTTP Post reminder interval. HTTP Post is sent once only.
reminder interval <minutes></minutes>	Sets the HTTP Post reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

http post (config-action-http_post:eth1 link state	change) level commands
clrscrn	Clears the screen.
	Enters the next lower level. Specify the instance for
connection <instance></instance>	the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the HTTP Post reminder interval. HTTP Post is sent once only.
reminder interval <minutes></minutes>	Sets the HTTP Post reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
http post (config-action-http_post:eth0 link state	change) level commands
clrscrn	Clears the screen.
connection <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
default mode	Sets default of simultaneous connection mode.
exit	Exits to the next higher level.
mode sequential	Sets sequential mode; will stop after first connection that goes through.
mode simultaneous	Sets simultaneous mode; will make all possible connections.
no reminder interval	Clears the HTTP Post reminder interval. HTTP Post is sent once only.
reminder interval <minutes></minutes>	Sets the HTTP Post reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
icmp (config-icmp) level commands	
clrscrn	Clears the screen.
exit	Exits to the configuration level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Prevents ICMP packets from being sent or received.
state enable	Allows ICMP packets to be sent and received.
write	Stores the current configuration in permanent memory.
if 1 (config-if:eth0) level commands	

bootp enable	Enables BOOTP.
clrscrn	Clears the screen.
default gateway <ip address=""></ip>	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
default priority	Restores the default priority for the interface.
dhcp client id <text></text>	Sets the DHCP client ID.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
domain <text></text>	Sets the domain name. <text> = name of the domain.</text>
exit	Exits to the config level.
failover	Enter failover configuration level
hostname <text></text>	Sets the host name. <text> = name of the host.</text>
if <instance></instance>	Changes to the interface configuration level.
ip address <ip address="" cidr=""></ip>	Sets the IP address and network mask. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
link	Enter link configuration level
mtu <bytes></bytes>	Sets the Maximum Transmission Unit (MTU) size.
no default gateway	Clears the default gateway.
no dhcp client id	Clears the DHCP client ID.
no domain	Clears the domain name.
no hostname	Clears the host name.
no ip address	Clears the IP address.
no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
primary dns <ip address=""></ip>	Sets the IP address of the primary DNS server.
priority <number></number>	Sets the priority for interface. <number> = priority number.</number>
secondary dns <ip address=""></ip>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show interface status
state disable	Disables the interface.
state enable	Enables the interface.
write	Stores the current configuration in permanent memory.
if 2 (config-if:eth1) level commands	
bootp disable	Disables BOOTP.
bootp enable	Enables BOOTP.
clrscrn	Clears the screen.
default gateway <ip address=""></ip>	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.

default priority	Restores the default priority for the interface.
dhcp client id <text></text>	Sets the DHCP client ID.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
domain <text></text>	Sets the domain name. <text> = name of the domain.</text>
exit	Exits to the config level.
failover	Enter failover configuration level
hostname <text></text>	Sets the host name. <text> = name of the host.</text>
if <instance></instance>	Changes to the interface configuration level.
ip address <ip address="" cidr=""></ip>	Sets the IP address and network mask. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
link	Enter link configuration level
mtu <bytes></bytes>	Sets the Maximum Transmission Unit (MTU) size.
no default gateway	Clears the default gateway.
no dhcp client id	Clears the DHCP client ID.
no domain	Clears the domain name.
no hostname	Clears the host name.
no ip address	Clears the IP address.
no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
primary dns <ip address=""></ip>	Sets the IP address of the primary DNS server.
priority <number></number>	Sets the priority for interface. <number> = priority number.</number>
secondary dns <ip address=""></ip>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show interface status
state disable	Disables the interface.
state enable	Enables the interface.
write	Stores the current configuration in permanent memory.

if 3 (config-if:eth2) level commands	
bootp disable	Disables BOOTP.
bootp enable	Enables BOOTP.
clrscrn	Clears the screen.
default gateway <ip address=""></ip>	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
default priority	Restores the default priority for the interface.
dhcp client id <text></text>	Sets the DHCP client ID.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
domain <text></text>	Sets the domain name. <text> = name of the domain.</text>

exit	Exits to the config level.
failover	Enter failover configuration level
hostname <text></text>	Sets the host name. <text> = name of the host.</text>
if <instance></instance>	Changes to the interface configuration level.
ip address <ip address="" cidr=""></ip>	Sets the IP address and network mask. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
link	Enter link configuration level
mtu <bytes></bytes>	Sets the Maximum Transmission Unit (MTU) size.
no default gateway	Clears the default gateway.
no dhcp client id	Clears the DHCP client ID.
no domain	Clears the domain name.
no hostname	Clears the host name.
no ip address	Clears the IP address.
no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
primary dns <ip address=""></ip>	Sets the IP address of the primary DNS server.
priority < <i>number</i> >	Sets the priority for interface. <number> = priority number.</number>
secondary dns <ip address=""></ip>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show interface status
state disable	Disables the interface.
state enable	Enables the interface.
write	Stores the current configuration in permanent memory.
ip (config-ip) level commands	
clrscrn	Clears the screen.
default ip time to live	Restores the default IP time to live.
default multicast time to live	Restores the default IP multicast time to live, which is one hop.
exit	Exits to the configuration level.
ip time to live <hops></hops>	Sets the IP time to live, known by SNMP as "ipDefaultTTL". <hops> = number of hops that a typical IP packet is allowed to live.</hops>
multicast time to live <hops></hops>	Sets the IP multicast time to live. <hops> = number of hops that a multicast IP packet is allowed to live.</hops>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
line 1 (line:1) level commands	
auto show statistics	Continuously displays line statistics.

baud rate <bits per="" second=""></bits>	Sets the line speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.

no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time
0	and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
•	Enters the configure-terminal level. line> = number
terminal < line>	of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char < <i>control</i> >	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char < <i>control</i> >	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 1 (config-consoleflow-line:1) level cor	
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default command delimiter	Restores the command delimiter.

default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.
line 2 (line:2) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. speeds standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <i><string></string></i>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 of hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
	D 1 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

default baud rate

default data bits

default parity default stop bits

default flow control

Restores the default speed of 9600 bits per second.

Restores the default of eight data bits.

Restores the default of no flow control. Restores the default of no parity.

Restores the default of one stop bit.

alada It the same land	Destance the feature defects the seekeld
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
ds
Clears the screen.
Sets the command delimiter.
Sets the firmware and configuration check interval.
Restores the command delimiter.
Restores the default firmware and configuration check interval.
Restores the default status update interval.
Exits to the config-consoleflow level.
Change to line configuration level.
Restores the default Project Tag.
Sets the Project Tag.
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
Disables command processing on line.
Enables command processing on line.
Sets the status update interval.
Stores the current configuration in permanent memory.
Continuously displays line statistics.
Sets the line speed. <bits per="" second=""> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.</bits>
Sets the serial counters to zero.
Clears the screen.
Sets the current line to always be in command mode.
Disables user-defined serial boot string to be echoed in the CLI.
Enables user-defined serial boot string to be echoed in the CLI.
Enables user to enter a custom string at boot time to enter command mode.
Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to</string>

	255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.

show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default command delimiter	Restores the command delimiter.
default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.
line 4 (line:4) level commands	
auto show statistics	Continuously displays line statistics.

baud rate <bits per="" second=""></bits>	Sets the line speed. standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.

no command mode	Disables command mode for the current line.
	Clears the signon message displayed at boot time
no command mode signon message	and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char < <i>control</i> >	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 4 (config-consoleflow-line:4) level co	
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default command delimiter	Restores the command delimiter.

default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.
line 5 (line:5) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. second> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
1.6.16.26	D

Restores the default of no parity.

Restores the default of one stop bit.

default parity

default stop bits

alafa It the wall all all	Destance the feeten defeath three held
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 5 (config-consoleflow-line:5) level comman	ds
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default command delimiter	Restores the command delimiter.
default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.
line 6 (line:6) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. <bits per="" second=""> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.</bits>
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to</string>

	255 or hex up to 0xFF. Within {} specify decimal
	milliseconds time delay.
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.

show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char < <i>control</i> >	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 6 (config-consoleflow-line:6) level c	ommands
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default command delimiter	Restores the command delimiter.
default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
	Otanas the assument and investigation in a second

write

Stores the current configuration in permanent

memory.

line 7 (line:7) level commands	
	Continuously displays line statistics
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
	(schar port) to be configured.

no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel < <i>line</i> >	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <i><control></control></i>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <pre>control</pre> C. A decimal value character has the form <pre>\mathbb{\text{99}}</pre> . A hex value character has the form <pre>0xFF</pre> .
xon char < <i>control</i> > line 7 (config-consoleflow-line:7) level co	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

line 7 (config-consoleflow-line:7) level commands	
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.

default command delimiter	Restores the command delimiter.
default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.

line 8 (line:8) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. <bits per="" second=""> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.</bits>
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.

default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	
	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.

write	Stores the current configuration in permanent memory.
xoff char < <i>control</i> >	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char < <i>control</i> >	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

line 8 (config-consoleflow-line:8) level commands	
clrscrn	Clears the screen.
command delimiter <text></text>	Sets the command delimiter.
content check interval <hours></hours>	Sets the firmware and configuration check interval.
default command delimiter	Restores the command delimiter.
default content check interval	Restores the default firmware and configuration check interval.
default status update interval	Restores the default status update interval.
exit	Exits to the config-consoleflow level.
line <number></number>	Change to line configuration level.
no project tag	Restores the default Project Tag.
project tag <text></text>	Sets the Project Tag.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables command processing on line.
state enable	Enables command processing on line.
status update interval <minutes></minutes>	Sets the status update interval.
write	Stores the current configuration in permanent memory.

line 9 (line:9) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.

command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.

show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal < <i>line</i> >	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <i><control></control></i>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 10 (line:10) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.

command mode serial string

command mode serial string <string>

Enables user to enter a custom string at boot time to

Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to

255 or hex up to 0xFF. Within {} specify decimal

enter command mode.

milliseconds time delay.

command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	
p	Uses no protocol on the line.
protocol tunnel	
•	Applies tunnel protocol on the line. Asserts line status with current configured values.
protocol tunnel	Applies tunnel protocol on the line. Asserts line status with current configured values.
protocol tunnel reassert	Applies tunnel protocol on the line.
protocol tunnel reassert show	Applies tunnel protocol on the line. Asserts line status with current configured values. Displays the current status. Shows the command mode settings for the current

show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

line 11 (line:11) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>

command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.

stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 12 (line:12) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure ourrent cottings	
configure current settings	Configures line with the current value of settings. Uses seven bits for data on the line.

data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.

threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 13 (line:13) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.

default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the actory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
now control none	Uses software (xon/xoff characters) flow control on
flow control software	the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel < <i>line</i> >	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.

write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 14 (line:14) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold default xoff char	Restores the factory default threshold. Restores the default xoff character on this line.
ueraur XVII Chai	restores the default xoll character on this line.

default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character

	has the form <control>C. A decimal value character</control>
	has the form \99. A hex value character has the form 0xFF.
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 15 (line:15) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. second> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of one stop bit
default stop bits default threshold	Restores the default of one stop bit. Restores the factory default threshold.
default trieshold default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
	1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal < <i>line</i> >	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>

xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
line 16 (line:16) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed. standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <string></string>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.</string>
command mode signon message <string></string>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
command mode wait time <milliseconds></milliseconds>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.</milliseconds>
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default parity	Restores the default of no parity.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the default welf above to an this line.
default von char	Restores the default xoff character on this line.
default xon char exit	Restores the default xon character on this line. Exits to the enable level
flow control hardware	
flow control none	Uses hardware (RTS/CTS) flow control on the line. Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.

gap timer <milliseconds></milliseconds>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
kill session	Kills command mode session on the Line
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
name <text></text>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <bytes></bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <control></control>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
xon char <control></control>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character

	has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
link (config-ethernet:eth2) level co	
clrscrn	Clears the screen.
default duplex	Restores the default duplex setting, which is auto.
default speed	Restores the default speed setting, which is autonegotiate.
duplex auto	Sets duplex mode to auto.
duplex full	Sets duplex mode to full.
duplex half	Sets duplex mode to half.
exit	Exit back to interface configuration level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
speed 10	Sets the speed of the Ethernet link to 10 Mbps.
speed 100	Sets the speed of the Ethernet link to 100 Mbps.
speed 1000	Sets the speed of the Ethernet link to 1000 Mbps.
speed auto	Sets the speed of the Ethernet link to autonegotiate.
write	Stores the current configuration in permanent memory.
link (config-ethernet:eth1) level co	ommands
clrscrn	Clears the screen.
default duplex	Restores the default duplex setting, which is auto.
default speed	Restores the default speed setting, which is autonegotiate.
duplex auto	Sets duplex mode to auto.
duplex full	Sets duplex mode to full.
duplex half	Sets duplex mode to half.
exit	Exit back to interface configuration level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
speed 10	Sets the speed of the Ethernet link to 10 Mbps.
speed 100	Sets the speed of the Ethernet link to 100 Mbps.
speed 1000	Sets the speed of the Ethernet link to 1000 Mbps.
speed auto	Sets the speed of the Ethernet link to autonegotiate.
write	Stores the current configuration in permanent memory.
link (config-ethernet:eth0) level co	•
clrscrn	Clears the screen.
default duplex	Restores the default duplex setting, which is auto.
	·
default speed	Restores the default speed setting, which is autonegotiate.
default speed duplex auto	Restores the default speed setting, which is autonegotiate. Sets duplex mode to auto.

duplex half	Sets duplex mode to half.
exit	Exit back to interface configuration level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
speed 10	Sets the speed of the Ethernet link to 10 Mbps.
speed 100	Sets the speed of the Ethernet link to 100 Mbps.
speed 1000	Sets the speed of the Ethernet link to 1000 Mbps.
speed auto	Sets the speed of the Ethernet link to autonegotiate.
write	Stores the current configuration in permanent memory.

log (config-diagnostics-log) level commands	
clrscrn	Clears the screen.
default max length	Restores the factory default maximum Log file size.
default output	Restores the default log output, which is disable.
default verbosity level	Restores the Verbosity level to the default value (Minimum).
exit	Exits to the next higher level.
max length <kbytes></kbytes>	Sets the maximum size in Kbytes for the Log file.
output disable	Disables log output.
output filesystem	Enables log to filesystem.
output line <number></number>	Enables log to serial line.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
verbosity level everything	Sets the Verbosity of system messages logs to the Syslog Host to Everything.
verbosity level intermediate	Sets the Verbosity of system messages logs to the Syslog Host to Intermediate .
verbosity level minimum	Sets the Verbosity of system messages logs to the Syslog Host to Minimum.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:16) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.

error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:15) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.

reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:14) level commar	nds
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.

write	Stores the current configuration in permanent memory.
modem (tunnel-modem:13) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:12) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.

echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:11) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.

incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:10) level comma	nds
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:9) level command	s
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

Clears the screen.

EDS-MD® Wired IoT Device Gateway Command Reference

clrscrn

connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:7) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.

echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:6) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.

no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:5) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.

verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:4) level command	ds
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address o the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:3) level command	ls .
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.

display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modern Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:2) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.

incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

modem (tunnel-modem:1) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem
Connect string <text></text>	emulation. <string> = connect string.</string>
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.

show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.

ntp (config-clock-ntp) level commands	
clrscrn	Clears the screen.
default server	Restores the default NTP server address.
exit	Exits to the next higher level.
server <text></text>	Sets the NTP server address.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

on scheduled reboot (config-action:on scheduled reboot)	
Clears the screen.	
Resets alarm processing delay to its default value.	
Sets the delay in processing the alarm. Alarm actions will not be executed if the cause is corrected within this time.	
Enters the next lower level.	
Exits to the config alarm level.	
Enters the next lower level.	
Enters the next lower level.	
Displays the current configuration.	
Displays the last 20 commands entered during the current CLI session.	
Displays statistics.	
Enters the next lower level.	
Stores the current configuration in permanent memory.	

packing (tunnel-packing:16) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.

packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

packing (tunnel-packing:15) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <control></control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

clrscrn default packing mode default send character default send character default threshold default timeout exit no trailing character packing mode disable Removes the send character for packing mode. Restores the default packing mode timeout. Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <centrol>C. A decimal value character has the form \(\text{Vent}\). Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeout value for packing mode in milliseconds. Sets the timeout value for packing mode. The character may be input as text, control, decimal, or hex. A control character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <centrol>C. A decimal value character has the form <cent< th=""><th>packing (tunnel-packing:14) level commands</th><th></th></cent<></centrol></centrol></centrol></centrol></centrol></centrol>	packing (tunnel-packing:14) level commands	
default send character Removes the send character for packing mode. default threshold Restores the default packing mode timeout. exit Returns to the tunnel level. no trailing character Removes the trailing character for packing mode. packing mode disable Disables packing. Data is sent to the network when received. Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). packing mode timeout Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <ont></ont>	clrscrn	Clears the screen.
default threshold default timeout Restores the default packing mode timeout. Returns to the tunnel level. Removes the trailing character for packing mode. Disables packing. Data is sent to the network when received. Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets he send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \99. A hex value character has the form \99. Commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeout value for packing mode. The character may be input as text, control, decimal, or hex. A control character for packing mode. The current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeout value for packing mode in milliseconds. <milliseconds. <milliseconds=""> = timeout value, in milliseconds. Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \square the form \square \square the form \square the</control></control></control></control></control></control></control></control></milliseconds.>	default packing mode	Sets to default packing mode, which is "Disable"
default timeout exit Returns to the tunnel level. Removes the trailing character for packing mode. Disables packing. Data is sent to the network when received. Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form 0xFF. show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeout value for packing mode in milliseconds. Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form <control>C. A decimal value character has the form <control>C. A decimal value character has the form write Stores the current configuration in permanent</control></control></control></control>	default send character	Removes the send character for packing mode.
exit no trailing character Removes the trailing character for packing mode. packing mode disable packing mode disable Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). packing mode timeout packing mode timeout Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <ontrol>C. A decimal value character has the form <ontrol>C. A decimal value character has the form <ontrol>C. A decimal value character has the form oxFF. Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. oytes> = number of bytes in the threshold. Sets the timeout value for packing mode in milliseconds. Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <ontrol>C. A decimal value character has the form <ontrol>C. A decim</ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol></ontrol>	default threshold	Restores the default threshold.
no trailing character packing mode disable packing mode disable packing mode disable packing mode send character packing mode send character packing mode send character packing mode timeout Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. \(< \cdot \) ytes> = number of bytes in the threshold. Sets the timeout value for packing mode in milliseconds. \(< \cdot \) milliseconds = timeout value, in milliseconds. Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A hex value character has the form \(\cdot \) A h	default timeout	Restores the default packing mode timeout.
Disables packing. Data is sent to the network when received. Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre>\control \in \text{C}\text{. A}\text{ decimal value character has the form \text{ Value character for packing mode in milliseconds.} Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre>\control C. A decimal value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the form \text{ V9. A hex value character has the for</pre></pre>	exit	Returns to the tunnel level.
packing mode disable received. Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port). Sets packing mode timeout Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre>\control</pre> send character <pre></pre> control> Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre>\control</pre> A control character has the form <pre>\control</pre> Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <pre></pre> <pre>\control <pre>Sets the timeout value for packing mode in milliseconds. Sets the timeout value for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre>\control</pre> character may be input as text, control, decimal, or hex. A control character has the form <pre>\control</pre> Character has the form <pre>\control</pre> Character has the form <pre>\control</pre> Sets the current configuration in permanent</pre></pre>	no trailing character	Removes the trailing character for packing mode.
packing mode send character it upon receiving the configured send character on the line (serial port). Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form <pre>N9. A hex value character has the form </pre> show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeout value for packing mode in milliseconds. Sets the timeout value for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form <control>C. A decimal value character has the form <pre>N9. A hex value character has the form <pre>N9. A hex value character has the form <pre>N9. A hex value character has the form </pre> Stores the current configuration in permanent</pre></pre></control></control></control>	packing mode disable	
it after a specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form \99. A hex value character has the form \square specified amount of time (timeout). Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \99. A hex value character has the form \99. A hex value character control> character for packing mode in milliseconds. <milliseconds. <control="" <milliseconds="timeout" as="" be="" character="" control,="" decimal,="" for="" in="" input="" may="" milliseconds.="" mode.="" or="" packing="" sets="" text,="" the="" trailing="" value,=""> character has the form <control> character has the form write Stores the current configuration in permanent</control></milliseconds.></control>	packing mode send character	it upon receiving the configured send character on
character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\). A hex value character has the form \(\formal{0xFF}\). Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeout value for packing mode in milliseconds. <milliseconds. <milliseconds=""> = timeout value, in milliseconds. Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\). The character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\). The character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\). The character has the form \(\formal{99}\). A hex value character has the form \(\formal{99}\).</control></milliseconds.></control>	packing mode timeout	
Show history Displays the last 20 commands entered during the current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. Sets the timeshold then the data will be sent. Sets the timeout value for packing mode in milliseconds. <milliseconds. <milliseconds=""> = timeout value, in milliseconds. <br< td=""><td>send character <control></control></td><td>character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex</control></td></br<></milliseconds.>	send character <control></control>	character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex</control>
current CLI session. Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <	show	Displays the current configuration.
threshold threshold threshold timeout <milliseconds> reaches this threshold then the data will be sent. </milliseconds>	show history	
timeout <milliseconds> milliseconds> = timeout value, in milliseconds. Sets the trailing character for packing mode. The character may be input as text, control, decimal, or trailing character <control> hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF. Stores the current configuration in permanent</control></control></milliseconds>	threshold <bytes></bytes>	reaches this threshold then the data will be sent.
character may be input as text, control, decimal, or trailing character <control> hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF. Stores the current configuration in permanent</control></control>	timeout <milliseconds></milliseconds>	milliseconds. <milliseconds> = timeout value, in</milliseconds>
WIII	trailing character < control>	character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex</control>
	write	

Clears the screen.

clrscrn

default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <control></control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold threshold threshold threshold threshold threshold threshold 	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:12) level command	s
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).

send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. cytes> = number of bytes in the threshold.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:11) level com	mands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmi it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmi it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.

timeout < milliseconds >

<bytes> = number of bytes in the threshold.
Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in

milliseconds.

trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:10) level com	mands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre><control>C</control></pre> . A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. cytes> = number of bytes in the threshold.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:9) level comm	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
Ψ/116	I Cotamo to the tannel level.

no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

packing (tunnel-packing:8) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <control></control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
threshold bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

	,
packing (tunnel-packing:7) level com	mands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

packing (tunnel-packing:6) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeshold default timeout	
exit	Restores the default packing mode timeout. Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. dytes> = number of bytes in the threshold.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:5) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).

packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <i><bytes></bytes></i>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout < <i>milliseconds</i> >	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < <i>control</i> >	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:4) level comr	nands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threehold	Destarce the default threehold

packing (tunnel-packing:4) level commands	
cirscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.

timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:3) level comm	nands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:2) level comm	nands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
	,

default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:1) level comn	nands
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.

packing (tunnel-packing:1) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character < control>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A</control>

	decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold bytes>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. dytes> = number of bytes in the threshold.
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character < control>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
write	Stores the current configuration in permanent memory.

password (tunnel-accept-password:16) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

password (tunnel-accept-password:15) level cor	nmands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

password (tunnel-accept-password:14) level co	ommands
cirscrn	Clears the screen.
exit	
exit	Exits to the next higher level. Removes the password so connections will be
no password	accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:13) level co	ommands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:12) level co	ommands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

password (tunnel-accept-password:11) level cor	nmands
cirscrn	Clears the screen.
exit	
exit	Exits to the next higher level. Removes the password so connections will be
no password	accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:10) level co	nmands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:9) level com	mands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

password (tunnel-accept-passy	vord:8) level commands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-passv	vord:7) level commands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-passv	vord:6) level commands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

password (tunnel-accept-password:	:5) level commands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:	:4) level commands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:	:3) level commands
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <text></text>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the
SHOW HIStory	current CLI session.

mands
Clears the screen.
Exits to the next higher level. Removes the password so connections will be
accepted unchallenged.
Sets the password required on the network side of the tunnel to begin a connection.
Inhibits any prompting for password on the network side of the tunnel.
Sets up so a user on the network side of the tunnel will be prompted for a password.
Shows the current configuration.
Displays the last 20 commands entered during the current CLI session.
Stores the current configuration in permanent memory.
mands
Clears the screen.
Exits to the next higher level.
Removes the password so connections will be accepted unchallenged.
Sets the password required on the network side of the tunnel to begin a connection.
Inhibits any prompting for password on the network side of the tunnel.
Sets up so a user on the network side of the tunnel will be prompted for a password.
Shows the current configuration.
Displays the last 20 commands entered during the current CLI session.
Stores the current configuration in permanent memory.
level commands
Clears the screen.
Restores the default value of the protocol (Both).
Exits to the config-gateway level.
Set the friendly name for port forwarding rule <text> = friendly name</text>
Sets the original WAN destination IP address for port forwarding rule.
Sets the LAN destination IP address for port forwarding rule.
Remove the friendly name.
Remove the friendly name. Clears the original WAN destination IP address for port forwarding rule.
Clears the original WAN destination IP address for

no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.

port forwarding rule 2 (config-portforwarding:	2) level commands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.
ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.
no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>

write	Stores the current configuration in permanent memory.
port forwarding rule 3 (config-portforwa	arding:3) level commands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.
ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.
no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.
port forwarding rule 4 (config-portforwa	arding:4) level commands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.
ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.

no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.

port forwarding rule 5 (config-portforwarding:5)	level commands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.
ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.
no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.

port forwarding rule 6 (config-portforwarding:6)	evel commands
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.
ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.
no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule <number></number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.

port forwarding rule 7 (config-portforwarding:7) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.

ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.
no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule < number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.
protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.

port forwarding rule 8 (config-portforwarding:8) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Both).
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for port forwarding rule <text> = friendly name</text>
ingress ip address <ip address=""></ip>	Sets the original WAN destination IP address for port forwarding rule.
ip address <ip address=""></ip>	Sets the LAN destination IP address for port forwarding rule.
no friendly name	Remove the friendly name.
no ingress ip address	Clears the original WAN destination IP address for port forwarding rule.
no ip address	Clears the LAN destination IP address for port forwarding rule.
no port or range	Clears the WAN port or range for port forwarding rule.
no target port	Clears the LAN destination port for port forwarding rule.
port forwarding rule < number>	Change to config gateway port forwarding level.
port or range <text></text>	Sets the WAN port or range for port forwarding rule. <text> = port or range.</text>
protocol both	Sets the protocol to Both (TCP and UDP).
protocol tcp	Sets the protocol to TCP.

protocol udp	Sets the protocol to UDP.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the port forwarding rule.
state enable	Enables the port forwarding rule.
target port <text></text>	Sets the LAN destination port for port forwarding rule. <text> = port.</text>
write	Stores the current configuration in permanent memory.

reboot schedule (device-reboot-schedule) level commands	
clrscrn	Clears the screen.
default hours	Restores the default hour of day for reboot schedule time.
default interval	Restores the default schedule interval.
default minutes	Restores the default minutes on the hour for reboot schedule.
default schedule	Restores the default reboot schedule type.
default unit	Restores the default reboot schedule interval unit.
exit	Returns to the previous level.
hours <hours></hours>	Sets the hour of day for reboot schedule (Use 24h time).
interval <number></number>	Sets the reboot schedule interval
minutes <minutes></minutes>	Sets the minutes on the hour for reboot schedule.
schedule daily	Sets the reboot schedule type to 'daily'.
schedule interval	Sets the reboot schedule type to 'interval'.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables scheduled reboots.
state enable	Enables scheduled reboots.
unit days	Sets the reboot schedule interval to days.
unit hours	Sets the reboot schedule interval to hours.
unit months	Sets the reboot schedule interval to months.
unit weeks	Sets the reboot schedule interval to weeks.
write	Stores the current configuration in permanent memory.

root level commands	
enable	Enters the enable level.
exit	Exit from the system
iperf <params></params>	Run iperf with command line parameters passed in quoted string.
ping <host></host>	Ping destination continuously with 5 second timeout
ping <host> <count></count></host>	Ping destination n times with 5 second timeout
ping <host> <count> <timeout></timeout></count></host>	Ping destination n times with x timeout (in seconds)
show	Show system information
show history	Displays the last 20 commands entered during the current CLI session.

show lines	Show line information
tcpdump <pre>cparameters></pre>	dump traffic on a network
trace route <host></host>	Trace route to destination
trace route <host> <protocol></protocol></host>	Trace route to destination using TCP, ICMP, or UDP

rss (config-rss) level commands	
clear rss	Clear the RSS Feed data
clrscrn	Clears the screen.
default max entries	Restores the default number of RSS feed entries.
exit	Exits to the configuration level.
feed disable	Disables RSS feed.
feed enable	Enables RSS feed.
max entries <number></number>	Sets the maximum number of RSS feed entries.
persist disable	Disables RSS feed data persistence.
persist enable	Enables RSS feed data persistence.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Display the RSS Feed status
write	Stores the current configuration in permanent memory.

serial (tunnel-serial:16) level commands	
cirscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.

serial (tunnel-serial:15) level commands	
cirscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:14) level command	ds
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:13) level command	ds
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:12) level command	ds
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:11) level command	ds .
cirscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:10) level command	ls .
cirscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:9) level commands	5
cirscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:8) level commands	3
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:7) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:6) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:5) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:4) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:3) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:2) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:1) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
server (ssh-server) level commands	
authorized user <username> <password></password></username>	Sets authorized username, password, and optionally RSA and/or DSA public keys
clrscrn	Clears the screen.
delete all authorized users	Removes all authorized users
delete authorized user <username></username>	Remove an authorized user
exit	Exits to the ssh level.
host generate dsa 1024	Generate DSA public and private keys
host generate dsa 512	Generate DSA public and private keys
host generate dsa 768	Generate DSA public and private keys
host generate rsa 1024	Generate RSA public and private keys
host generate rsa 512	Generate RSA public and private keys

host generate rsa 768	Generate RSA public and private keys
host keys	Sets RSA or DSA public and/or private keys
no host dsa	Removes DSA public and private keys
no host rsa	Removes RSA public and private keys
show	Show SSH Server settings
show authorized user <username></username>	Show information for an authorized user
show history	Displays the last 20 commands entered during the current CLI session.
show host dsa	Show full DSA public key
show host rsa	Show full RSA public key
write	Stores the current configuration in permanent memory.

smtp (config-smtp) level commands	
cirscrn	Clears the screen.
default server port	Restores the SMTP server port to its default.
exit	Exits to the configuration level.
from address <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
no from address	Removes the From address for email alerts.
no overriding domain	Removes the overriding domain name option.
no password	Removes the password.
no server address	Removes the SMTP server address.
no username	Removes the username.
overriding domain <text></text>	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the deviceÂ's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
password <text></text>	Sets the password for logging in to the mail server.
server address <text></text>	Sets an SMTP server address to direct all outbound email messages through a mail server.
server port <number></number>	Sets the SMTP server port.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets the username for logging in to the mail server.
write	Stores the current configuration in permanent memory.

snmp (config-snmp) level commar	nds
clrscrn	Clears the screen.
exit	Returns to the config level.
no system location	Clears the SNMP system location.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays the SNMP agent status.
snmpd	Enters the next lower level.

system location <text></text>	Sets the SNMP system location. <text> = location of device.</text>
traps	Enters the next lower level.
write	Stores the current configuration in permanent memory.
snmp trap (config-action-snmp_trap:on	scheduled reboot) level commands
alarm message <text></text>	Sets the message to be sent when the alarm turns on.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no alarm message	Removes the alarm message.
no normal message	Removes the normal message.
no reminder interval	Clears the SNMP Trap reminder interval. SNMP Trap is sent once only.
normal message <text></text>	Sets the message to be sent when the alarm turns off.
reminder interval <minutes></minutes>	Sets the SNMP Trap reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Does not send SNMP Trap.
state enable	Sends SNMP Trap when alarm condition is met.
	Stores the current configuration in permanent
write	memory.
write snmp trap (config-action-snmp_trap:eth	memory.
	memory.
snmp trap (config-action-snmp_trap:eth	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns
<pre>snmp trap (config-action-snmp_trap:eth alarm message <text></text></pre>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit</text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on.
<pre>snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn</text></pre>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message</text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message</text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval</text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text></text></text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes></minutes></text></text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes> show</minutes></text></text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval. Shows the current configuration. Displays the last 20 commands entered during the
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes> show show history</minutes></text></text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval. Shows the current configuration. Displays the last 20 commands entered during the current CLI session.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes> show show history state disable</minutes></text></text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Does not send SNMP Trap.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes> show show history state disable state enable</minutes></text></text>	memory. Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Does not send SNMP Trap. Sends SNMP Trap when alarm condition is met. Stores the current configuration in permanent memory.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes> show show history state disable state enable write</minutes></text></text>	memory. Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Does not send SNMP Trap. Sends SNMP Trap when alarm condition is met. Stores the current configuration in permanent memory.
snmp trap (config-action-snmp_trap:eth alarm message <text> clrscrn exit no alarm message no normal message no reminder interval normal message <text> reminder interval <minutes> show show history state disable state enable write snmp trap (config-action-snmp_trap:eth</minutes></text></text>	memory. 2 link state change) level commands Sets the message to be sent when the alarm turns on. Clears the screen. Exits to the next higher level. Removes the alarm message. Removes the normal message. Clears the SNMP Trap reminder interval. SNMP Trap is sent once only. Sets the message to be sent when the alarm turns off. Sets the SNMP Trap reminder interval. Shows the current configuration. Displays the last 20 commands entered during the current CLI session. Does not send SNMP Trap. Sends SNMP Trap when alarm condition is met. Stores the current configuration in permanent memory. 1 link state change) level commands Sets the message to be sent when the alarm turns

no alarm message	Removes the alarm message.
no normal message	Removes the normal message.
no reminder interval	Clears the SNMP Trap reminder interval. SNMP Trap is sent once only.
normal message <text></text>	Sets the message to be sent when the alarm turns off.
reminder interval <minutes></minutes>	Sets the SNMP Trap reminder interval.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Does not send SNMP Trap.
state enable	Sends SNMP Trap when alarm condition is met.
write	Stores the current configuration in permanent memory.

snmpd (config-snmp-snmpd) level commands	
authentication password <text></text>	Sets password used for authentication for agent.
authentication protocol md5	Uses MD5 for authentication for agent.
authentication protocol sha	Uses SHA for authentication for agent.
clrscrn	Clears the screen.
default authentication protocol	Restores to default SNMPv3 authentication method: MD5 for agent.
default privacy protocol	Restores to default SNMPv3 privacy encryption method: DES for agent.
default read community	Restores the SNMP read-only community to default: public
default security	Restores to default SNMPv3 security method: Authentication, No Privacy for agent.
default system description	Restores the SNMP system description to its default.
default system name	Restores the SNMP system name to default: the product name.
default version	Restores to default SNMP version v2c for agent.
default write community	Clears the SNMP read/write community to default: private
exit	Exits to the next higher level.
no authentication password	Clears authentication password for agent.
no privacy password	Clears privacy password for agent.
no system contact	Clears the SNMP system contact.
no username	Clears SNMPv3 username for agent.
privacy password <text></text>	Sets password used for privacy encryption for agent.
privacy protocol aes	Uses AES for privacy encryption for agent.
privacy protocol des	Uses DES for privacy encryption for agent.
read community <text></text>	Sets the SNMP read-only community string. <text> = name of the read-only community string to be set.</text>
security authentication and privacy	Authentication and Privacy for agent.
security authentication but no privacy	Authentication, No Privacy for agent.
security no authentication and no priv	No Authentication, No Privacy for agent.
show	Shows the current configuration.

show history Displays the last 20 commands entered during the current CLI session. State disable Disables the SNMP agent. Enables the SNMP agent. Sets the SNMP agent. Sets the SNMP system contact information. <text> = system contact information. Sets the SNMP system description. <text> = system contact information. Sets the SNMP system description. <text> = description of device. System name <text></text></text></text></text>		
show history current CLI session. Solores the current configuration level. Displays the active commands client Enters the SSH Server configuration in permanent memory. Solores the default port solored for current configuration in permanent memory. Solores the current configuration level. Clears the SSH Server configuration level. Clears the screen. Solores the current configuration level. Clears the commands entered during the current CLI session. Solores the current configuration in permanent memory. Solores the default maximum allowed concurrent incoming SSH sessions. Solores the default coal port to the SSH server. Exits to the CLI level. Solores the current configuration. Solores the current configuration in permanent memory.	show engine id	Displays the SNMP agent engine ID.
state enable Sets the SNMP agent. Sets the SNMP system contact information. <text> system contact information. <text> system contact information. Sets the SNMP system description <text> description of device. Sets the SNMP system name. <text> = description of device. Sets the SNMP system name. <text> = SSM system configuration in permanent memory. <text> = same of the read-write community string. <text> = name of the read-write comfiguration level. <text> = SSM (ssh) level commands entered during the current CLI session. <text> = String system sys</text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text>	show history	
Sets the SNMP system contact information. <text> system contact information. <text> system contact information. <text> system contact information. <text> Sets the SNMP system description. <text> description of device. Sets the SNMP system name. <text> Sets the SNMP system name. <text> = SNMP system name. Sets SNMPv3 username for agent. Version snmpv1 Version snmpv2 Version snmpv2 Version snmpv3 Uses SNMPv3 for agent. Version snmpv3 Uses SNMPv3 for agent. Version snmpv4 Version snmpv4 Version snmpv4 Version snmpv5 Version snmpv6 Version snmpv7 Version snmpv7 Version snmpv7 Version snmpv7 Version snmpv7 Version snmpv8 Version snmpv8 Version snmpv8 Version snmpv8 Version snmpv8 Version snmpv9 Version snmpv9 Version snmpv9 Version snmpv9 Version snmpv9 Version snmpv8 Version snmpv8 Version snmpv9 Version snmpv8 Version snmpv8 Version snmpv8 Version snmpv9 Version s</text></text></text></text></text></text></text>	state disable	Disables the SNMP agent.
system contact information. system description <text> system name description <text> system name <text> system name <text> sets the SNMP system and system name. <text> = SNMP system name. system name <text> sets SNMPv3 username for agent. version snmpv1 Uses SNMPv2 for agent. version snmpv2c version snmpv3 Uses SNMPv3 for agent. version snmpv3 version snmpv3 Version snmpv3 Version snmpv4 version snmpv5 version snmpv6 version snmpv7 Version snmpv7 Version snmpv8 version snmpv8 version snmpv9 Version spmpv1 Version snmpv9 Version spmpv1 Version spmpv1 Version spmpv1 Version spmpv1 Version spmpv2 Version spmpv1 Version spmpv1 Version spmpv2 Version spmpv1 Versio</text></text></text></text></text></text>	state enable	
description of device. system name <text> Sets the SNMP system name. <text> = SNMP system name. system name. system name. system name. sers SNMPv3 username for agent. version snmpv1 Uses SNMPv2c for agent. version snmpv3 Uses SNMPv3 for agent. version snmpv3 Uses SNMPv3 for agent. write Stores the current configuration in permanent memory. write community <text> Sets the SNMP read-write community string. <text> = name of the read-write community string to be set. ssh (ssh) level commands client client client sthe SSH Client configuration level. client client Exits to the enable level. server Sets the SSH Server configuration level. Displays the last 20 commands entered during the current current current incoming SSH sessions. <number> show history clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. default port Restores the default local port to the SSH server. show Sets the CLI level. Sets the CLI level. Sets the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. show Displays the last 20 commands entered during the current Configuration. Displays the last 20 commands entered during the current Configuration. Displays the last 20 commands entered during the current Configuration. Displays the last 20 commands entered during the current Configuration. Displays the last 20 commands entered during the current Configuration. Displays the last 20 commands entered during the current Configuration in permanent memory. Solves the current configuration in permanent memory.</number></number></number></text></text></text></text>	system contact <text></text>	Sets the SNMP system contact information. <text> = system contact information.</text>
system name. username <text></text>	system description <text></text>	description of device.
version snmpv1 version snmpv2c Uses SNMPv2 for agent. version snmpv3 Uses SNMPv3 for agent. write Stores the current configuration in permanent memory. Sets the SNMP read-write community string, <text>= name of the read-write community string to be set. Ssh (ssh) level commands client Enters the SSH Client configuration level. Clears the screen. exit Exits to the enable level. Show history Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. Ssh (config-cli-ssh) level commands cliscrn Clears the screen. Exits to the enable level. Stores the default maximum allowed concurrent incoming SSH sessions. Clears the screen. Gefault max sessions default port Restores the default local port to the SSH server. exit Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. Sets the local port that the SSH server uses. <number> = local port number. show Displays the local port that the SSH server uses. <number> = local port number. Displays the last 20 commands entered during the current cur</number></number></number></text>	system name <text></text>	
version snmpv2c version snmpv3 Uses SNMPv2c for agent. write Stores the current configuration in permanent memory. write community <text> Sets the SNMP read-write community string, <text> = name of the read-write community string to be set. Ssh (ssh) level commands client Client Clears the screen. exit Exits to the enable level. server Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. Write Stores the current configuration in permanent memory. Ssh (config-cli-ssh) level commands clirscrn Clears the screen. Glears the screen. Clears the screen. Gleauth max sessions Clears the default maximum allowed concurrent incoming SSH sessions. Glefault port Restores the default local port to the SSH server. exit Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> sets the local port to the SSH server sets the local port to the SSH server. Exits to the CLI level. Sets the local port that the SSH server uses. <number> show Displays the current configuration. Displays the current configuration. Displays the sSH server statistics. Displays the SSH server. Enables the SSH Server. Enables the SSH Server. Stores the current configuration in permanent memory.</number></number></text></text>	username <text></text>	
write Stores the current configuration in permanent memory. write community <text></text>	version snmpv1	-
write Stores the current configuration in permanent memory. write community <text> Sets the SNMP read-write community string, <text> = name of the read-write community string to be set. Ssh (ssh) level commands client Enters the SSH Client configuration level. clrscrn Clears the screen. exit Exits to the enable level. server Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. write Stores the current configuration in permanent memory. Ssh (config-cli-ssh) level commands clrscrn Clears the screen. default max sessions default port Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. max sessions <number> sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. sets the local port that the SSH server uses. <number> = local port number. show Displays the current configuration. Displays the current configuration. Displays the sSH server statistics. Displays the SSH server statistics. Displays the SSH Server. state enable Enables the SSH Server. write Stores the current configuration in permanent memory.</number></number></number></text></text>	version snmpv2c	
write community <text> sets the SNMP read-write community string, <text> = name of the read-write community string to be set. Ssh (ssh) level commands client Clears the SSH Client configuration level. Clears the screen. exit Exits to the enable level. Server Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. Ssh (config-cli-ssh) level commands clrscm Clears the screen. Clears the screen. Clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. sets the local port that the SSH server uses. <number> = local port number. Sets the local port that the SSH server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Displays the SSH server statistics. Displays the SSH server statistics. Displays the SSH server. Stores the SSH Server. Stores the current configuration in permanent memory. SSI (ssl) level commands</number></number></number></text></text>	version snmpv3	
### continuity <texts ###="" be="" community="" of="" read-write="" s<="" set="" set.="" string="" td="" the="" to="" ="name"><td>write</td><td></td></texts>	write	
client clrscrn clears the SSH Client configuration level. Clears the screen. Exits to the enable level. Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. Write Stores the current configuration in permanent memory. SSH (config-cli-ssh) level commands Clrscrn Clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. Restores the default local port to the SSH server. Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> Sets the local port that the SSH server uses. <number> = local port number. Show Displays the current configuration. Displays the SSH server statistics. Displays the SSH server. state disable Disables the SSH Server. Stores the current configuration in permanent memory. SSI (ssI) level commands</number></number></number>	write community <text></text>	Sets the SNMP read-write community string. <text> = name of the read-write community string to be set.</text>
clrscrn exit Exits to the enable level. Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. SSh (config-cli-ssh) level commands clrscrn Clears the screen. default max sessions Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. max sessions <number> Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Displays the SSH server statistics. State disable Disables the SSH Server. Enables the SSH Server. Stores the current configuration in permanent memory. SSI (ssI) level commands</number></number></number>	ssh (ssh) level commands	
clrscrn exit Exits to the enable level. Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. SSh (config-cli-ssh) level commands clrscrn Clears the screen. default max sessions Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. max sessions <number> Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Displays the SSH server statistics. State disable Disables the SSH Server. Enables the SSH Server. Stores the current configuration in permanent memory. SSI (ssI) level commands</number></number></number>	client	Enters the SSH Client configuration level.
Enters the SSH Server configuration level. Displays the last 20 commands entered during the current CLI session. Write Stores the current configuration in permanent memory. Ssh (config-cli-ssh) level commands Clrscrn Clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> Sets the local port that the SSH server uses. <number> = local port number. show Displays the last 20 commands entered during the current CLI session. Show statistics Displays the SSH server statistics. Displays the SSH server. State disable Stores the current configuration in permanent memory. State (sst) level commands</number></number></number>	clrscrn	3
show history Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. SSh (config-cli-ssh) level commands Clescrn Clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. max sessions <number> Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> show Displays the current configuration. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics Displays the SSH server statistics. state disable Disables the SSH Server. state enable Enables the SSH Server. Stores the current configuration in permanent memory.</number></number></number>	exit	Exits to the enable level.
show history Displays the last 20 commands entered during the current CLI session. Stores the current configuration in permanent memory. SSh (config-cli-ssh) level commands Clescrn Clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. default port Restores the default local port to the SSH server. exit Exits to the CLI level. max sessions <number> Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> show Displays the current configuration. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. show statistics Displays the SSH server statistics. state disable Disables the SSH Server. state enable Enables the SSH Server. Stores the current configuration in permanent memory.</number></number></number>	server	Enters the SSH Server configuration level.
ssh (config-cli-ssh) level commands clrscrn Clears the screen. Restores the default maximum allowed concurrent incoming SSH sessions. default port exit Exits to the CLI level. max sessions <number> Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> show Displays the current configuration. bisplays the last 20 commands entered during the current CLI session. Displays the SSH server statistics. state disable Disables the SSH Server. Stores the current configuration in permanent memory. SSI (SSI) level commands</number></number></number>	show history	Displays the last 20 commands entered during the
clrscrn default max sessions default port exit max sessions port port </td <td>write</td> <td></td>	write	
default max sessions default port default port exit max sessions < number> port < number> show show history show statistics state enable write Restores the default maximum allowed concurrent incoming Restores the default local port to the SSH server. Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. Sets the local port that the SSH server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Displays the SSH server statistics. Disables the SSH Server. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory.</number></number>	ssh (config-cli-ssh) level commands	
default max sessions default port default port exit max sessions < number> port < number> show show history show statistics state enable write Restores the default maximum allowed concurrent incoming Restores the default local port to the SSH server. Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. Sets the local port that the SSH server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Displays the SSH server statistics. Disables the SSH Server. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory.</number></number>		Clears the screen
default port exit Exits to the CLI level. Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> Sets the local port that the SSH server uses. <number> = local port number. Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Displays the SSH server statistics. Displays the SSH Server. State disable Disables the SSH Server. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory.</number></number></number>	default max sessions	Restores the default maximum allowed concurrent
exit max sessions <number> Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions. port <number> port <number> Sets the local port that the SSH server uses. <number> = local port number. Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Displays the SSH server statistics. Displays the SSH Server. State disable Disables the SSH Server. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory.</number></number></number></number></number>	default port	
max sessions <number> SSH sessions. <number> = number of sessions. Sets the local port that the SSH server uses. <number> = local port number. Show Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Show statistics Displays the SSH server statistics. Displays the SSH Server. State disable Disables the SSH Server. State enable Enables the SSH Server. Stores the current configuration in permanent memory. SSI (SSI) level commands</number></number></number>		·
<pre>cnumber> = local port number. show</pre>	max sessions < <i>number</i> >	
show history Show statistics State disable State enable Write Displays the last 20 commands entered during the current CLI session. Displays the SSH server statistics. Displays the SSH server statistics. Displays the SSH server statistics. Stores the SSH Server. Stores the SSH Server. Stores the current configuration in permanent memory. SSI (SSI) level commands	port <number></number>	
show history current CLI session. Displays the SSH server statistics. State disable Disables the SSH Server. State enable Enables the SSH Server. Stores the current configuration in permanent memory. SSI (SSI) level commands	show	Displays the current configuration.
state disable state enable state enable write Disables the SSH Server. Enables the SSH Server. Stores the current configuration in permanent memory. Stores the current configuration in permanent memory.	show history	
state enable write Enables the SSH Server. Stores the current configuration in permanent memory. ssl (ssl) level commands	show statistics	Displays the SSH server statistics.
write Stores the current configuration in permanent memory. ssl (ssl) level commands	state disable	Disables the SSH Server.
memory. ssi (ssi) level commands	state enable	Enables the SSH Server.
	write	
clrscrn Clears the screen.	ssl (ssl) level commands	
	clrscrn	Clears the screen.

credentials	Enters the SSL credentials configuration level.
exit	Exits to the enable level.
show history	Displays the last 20 commands entered during the current CLI session.
trusted authorities	Enters the SSL configuration level.
write	Stores the current configuration in permanent memory.
static leases 1 (config-dhcpd-static_leases:1) le	evel commands
clrscrn	Clears the screen.
exit	Exits to the config-dhcpd level.
ip address <ip address=""></ip>	Sets the reserved IP address.
mac address < hexadecimal>	Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
no ip address	Clears the reserved IP address.
no mac address	Removes the MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
static leases < number>	Change to dhcpd static lease level.
write	Stores the current configuration in permanent
WIILE	memory.
	memory. evel commands
static leases 2 (config-dhcpd-static_leases:2) le	evel commands
static leases 2 (config-dhcpd-static_leases:2) le	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address.
static leases 2 (config-dhcpd-static_leases:2) leasern exit	Clears the screen. Exits to the config-dhcpd level.
static leases 2 (config-dhcpd-static_leases:2) leases:2)	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal>	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address.
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address.
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address show	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address. Displays the current configuration. Displays the last 20 commands entered during the
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address show show history	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address. Displays the current configuration. Displays the last 20 commands entered during the current CLI session.
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address show show history static leases < number>	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Change to dhcpd static lease level. Stores the current configuration in permanent memory.
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address show show history static leases < number> write	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Change to dhcpd static lease level. Stores the current configuration in permanent memory.
static leases 2 (config-dhcpd-static_leases:2) lectrorn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address show show history static leases < number> write static leases 3 (config-dhcpd-static_leases:3) lectrory	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Change to dhcpd static lease level. Stores the current configuration in permanent memory.
static leases 2 (config-dhcpd-static_leases:2) lectrscrn exit ip address < IP address> mac address < hexadecimal> no ip address no mac address show show history static leases < number> write static leases 3 (config-dhcpd-static_leases:3) lectrscrn	Clears the screen. Exits to the config-dhcpd level. Sets the reserved IP address. Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces. Clears the reserved IP address. Removes the MAC Address. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Change to dhcpd static lease level. Stores the current configuration in permanent memory.

	3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that
no in address	quotes must enclose the value if it contains spaces. Clears the reserved IP address.
no ip address no mac address	Removes the MAC Address.
show	
SHOW	Displays the current configuration. Displays the last 20 commands entered during the
show history	current CLI session.
static leases <number></number>	Change to dhcpd static lease level.
write	Stores the current configuration in permanent memory.
static leases 4 (config-dhcpd-static_le	ases:4) level commands
clrscrn	Clears the screen.
exit	Exits to the config-dhcpd level.
ip address <ip address=""></ip>	Sets the reserved IP address.
	Sets the MAC Address. Each byte is represented by
mac address < hexadecimal>	two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
no ip address	Clears the reserved IP address.
no mac address	Removes the MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
static leases < number>	Change to dhcpd static lease level.
write	Stores the current configuration in permanent memory.
static leases 5 (config-dhcpd-static_le	ases:5) level commands
clrscrn	Clears the screen.
exit	Exits to the config-dhcpd level.
ip address <ip address=""></ip>	Sets the reserved IP address.
mac address < hexadecimal>	Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
no ip address	Clears the reserved IP address.
no mac address	Removes the MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
static leases <number></number>	Change to dhcpd static lease level.
write	Stores the current configuration in permanent memory.
static leases 6 (config-dhcpd-static_le	ases:6) level commands
clrscrn	Clears the screen.
exit	Exits to the config-dhcpd level.
	i

Sets the reserved IP address.

ip address <IP address>

mac address < <i>hexadecimal</i> >	Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
no ip address	Clears the reserved IP address.
no mac address	Removes the MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
static leases <number></number>	Change to dhcpd static lease level.
vrite	Stores the current configuration in permanent memory.
static leases 7 (config-dhcpd-static_leases:7)	level commands
clrscrn	Clears the screen.
exit	Exits to the config-dhcpd level.
p address	Sets the reserved IP address.
mac address <i><hexadecimal></hexadecimal></i>	Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
no ip address	Clears the reserved IP address.
no mac address	Removes the MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
static leases <number></number>	Change to dhcpd static lease level.
vrite	Stores the current configuration in permanent memory.
static leases 8 (config-dhcpd-static_leases:8)	level commands
clrscrn	Clears the screen.
exit	Exits to the config-dhcpd level.
p address <ip address=""></ip>	Sets the reserved IP address.
mac address < hexadecimal>	Sets the MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
no ip address	Clears the reserved IP address.
no mac address	Removes the MAC Address.
show	Displays the current configuration.
	Displays the last 20 commands entered during the current CLI session.
show history	Current CEI Session.
show history static leases < <i>number</i> >	Change to dhcpd static lease level.

Clears the screen.

clrscrn

default metric	Restores the metric to default value.
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>
gateway <text></text>	Sets the gateway for static route network.
interface <text></text>	Sets the route interface <text> = interface name</text>
metric <number></number>	Sets the metric for static route. <number> = metric</number>
network <text></text>	Sets the IP address and network mask for static route network.
no friendly name	Remove the friendly name
no gateway	Clears the gateway for static route network.
no interface	Clears the route interface. The WAN interface is used if no interface is specified.
no network	Clears the IP address for static route network.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the static route.
state enable	Enables the static route.
static route < number>	Change to config gateway static route level.
write	Stores the current configuration in permanent memory.

static route 2 (config-staticroute:2) level commands		
clrscrn	Clears the screen.	
default metric	Restores the metric to default value.	
exit	Exits to the config-gateway level.	
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>	
gateway <text></text>	Sets the gateway for static route network.	
interface <text></text>	Sets the route interface <text> = interface name</text>	
metric <number></number>	Sets the metric for static route. <number> = metric</number>	
network <text></text>	Sets the IP address and network mask for static route network.	
no friendly name	Remove the friendly name	
no gateway	Clears the gateway for static route network.	
no interface	Clears the route interface. The WAN interface is used if no interface is specified.	
no network	Clears the IP address for static route network.	
show	Displays the current configuration.	
show history	Displays the last 20 commands entered during the current CLI session.	
state disable	Disables the static route.	
state enable	Enables the static route.	
static route < number>	Change to config gateway static route level.	
write	Stores the current configuration in permanent memory.	

static route 3 (config-staticroute:3) level commands	
clrscrn	Clears the screen.

default metric	Restores the metric to default value.
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>
gateway <text></text>	Sets the gateway for static route network.
interface <text></text>	Sets the route interface <text> = interface name</text>
metric <number></number>	Sets the metric for static route. <number> = metric</number>
network <text></text>	Sets the IP address and network mask for static route network.
no friendly name	Remove the friendly name
no gateway	Clears the gateway for static route network.
no interface	Clears the route interface. The WAN interface is used if no interface is specified.
no network	Clears the IP address for static route network.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the static route.
state enable	Enables the static route.
static route < number>	Change to config gateway static route level.
write	Stores the current configuration in permanent memory.

static route 4 (config-staticroute:4) level commands		
clrscrn	Clears the screen.	
default metric	Restores the metric to default value.	
exit	Exits to the config-gateway level.	
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>	
gateway <text></text>	Sets the gateway for static route network.	
interface <text></text>	Sets the route interface <text> = interface name</text>	
metric <number></number>	Sets the metric for static route. <number> = metric</number>	
network <text></text>	Sets the IP address and network mask for static route network.	
no friendly name	Remove the friendly name	
no gateway	Clears the gateway for static route network.	
no interface	Clears the route interface. The WAN interface is used if no interface is specified.	
no network	Clears the IP address for static route network.	
show	Displays the current configuration.	
show history	Displays the last 20 commands entered during the current CLI session.	
state disable	Disables the static route.	
state enable	Enables the static route.	
static route < number>	Change to config gateway static route level.	
write	Stores the current configuration in permanent memory.	

static route 5 (config-staticroute:5) level commands	
clrscrn	Clears the screen.

Restores the metric to default value.
Exits to the config-gateway level.
Set the friendly name for static route. <text> = friendly name</text>
Sets the gateway for static route network.
Sets the route interface <text> = interface name</text>
Sets the metric for static route. <number> = metric</number>
Sets the IP address and network mask for static route network.
Remove the friendly name
Clears the gateway for static route network.
Clears the route interface. The WAN interface is used if no interface is specified.
Clears the IP address for static route network.
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
Disables the static route.
Enables the static route.
Change to config gateway static route level.
Stores the current configuration in permanent memory.

static route 6 (config-staticroute:6) level commands		
clrscrn	Clears the screen.	
default metric	Restores the metric to default value.	
exit	Exits to the config-gateway level.	
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>	
gateway <text></text>	Sets the gateway for static route network.	
interface <text></text>	Sets the route interface <text> = interface name</text>	
metric <number></number>	Sets the metric for static route. <number> = metric</number>	
network <text></text>	Sets the IP address and network mask for static route network.	
no friendly name	Remove the friendly name	
no gateway	Clears the gateway for static route network.	
no interface	Clears the route interface. The WAN interface is used if no interface is specified.	
no network	Clears the IP address for static route network.	
show	Displays the current configuration.	
show history	Displays the last 20 commands entered during the current CLI session.	
state disable	Disables the static route.	
state enable	Enables the static route.	
static route < number>	Change to config gateway static route level.	
write	Stores the current configuration in permanent memory.	

static route 7 (config-staticroute:7) level	commands
clrscrn	Clears the screen.

default metric	Restores the metric to default value.
exit	Exits to the config-gateway level.
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>
gateway <text></text>	Sets the gateway for static route network.
interface <text></text>	Sets the route interface <text> = interface name</text>
metric <number></number>	Sets the metric for static route. <number> = metric</number>
network <text></text>	Sets the IP address and network mask for static route network.
no friendly name	Remove the friendly name
no gateway	Clears the gateway for static route network.
no interface	Clears the route interface. The WAN interface is used if no interface is specified.
no network	Clears the IP address for static route network.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the static route.
state enable	Enables the static route.
static route <number></number>	Change to config gateway static route level.
write	Stores the current configuration in permanent memory.

static route 8 (config-staticroute:8) level commands		
clrscrn	Clears the screen.	
default metric	Restores the metric to default value.	
exit	Exits to the config-gateway level.	
friendly name <text></text>	Set the friendly name for static route. <text> = friendly name</text>	
gateway <text></text>	Sets the gateway for static route network.	
interface <text></text>	Sets the route interface <text> = interface name</text>	
metric <number></number>	Sets the metric for static route. <number> = metric</number>	
network <text></text>	Sets the IP address and network mask for static route network.	
no friendly name	Remove the friendly name	
no gateway	Clears the gateway for static route network.	
no interface	Clears the route interface. The WAN interface is used if no interface is specified.	
no network	Clears the IP address for static route network.	
show	Displays the current configuration.	
show history	Displays the last 20 commands entered during the current CLI session.	
state disable	Disables the static route.	
state enable	Enables the static route.	
static route <number></number>	Change to config gateway static route level.	
write	Stores the current configuration in permanent memory.	

Clears the screen.

-DS-MD(R)	Wired In I	Device	Gateway (Command	Reference

syslog (config-syslog) level commands

clrscrn

default remote port	Restores the default syslog remote port.
default severity log level	No logging.
exit	Returns to the config level.
host <text></text>	Sets the address of the syslog recipient. <text> = IP address or name of the host.</text>
no host	Removes the address of the syslog recipient.
remote port <number></number>	Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.</number>
severity log level alert	Log only Alert and more severe events.
severity log level critical	Log only Critical and more severe events.
severity log level debug	Log all events.
severity log level emergency	Log only Emergency events.
severity log level error	Log only Error and more severe events.
severity log level information	Log only Information and more severe events.
severity log level none	No logging.
severity log level notice	Log only Notice and more severe events.
severity log level warning	Log only Warning and more severe events.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the syslog statistics.
state disable	Disables syslog logging.
state enable	Enables syslog logging.
write	Stores the current configuration in permanent memory.
telnet (config-cli-telnet) level commands	
authentication disable	No password required for Telnet users.
authentication enable	Challenges the Telnet user with a password.
clrscrn	Clears the screen.
lefe line energy	
default max sessions	Restores the default maximum allowed concurrent incoming Telnet sessions.
default port	
	incoming Telnet sessions.
default port	incoming Telnet sessions. Restores the default local port to the Telnet server.
default port exit	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming
default port exit max sessions < number>	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions. Sets the local port that the Telnet server uses.</number>
default port exit max sessions < number> port < number>	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions. Sets the local port that the Telnet server uses. <number> = local port number.</number></number>
default port exit max sessions < number> port < number> show	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions. Sets the local port that the Telnet server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the</number></number>
default port exit max sessions < number> port < number> show show history	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions. Sets the local port that the Telnet server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the current CLI session.</number></number>
default port exit max sessions < number> port < number> show show history show statistics	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions. Sets the local port that the Telnet server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Displays the Telnet statistics.</number></number>
default port exit max sessions <number> port <number> show show history show statistics state disable</number></number>	incoming Telnet sessions. Restores the default local port to the Telnet server. Exits to the CLI level. Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions. Sets the local port that the Telnet server uses. <number> = local port number. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Displays the Telnet statistics. Disables the Telnet Server.</number></number>

break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break < <i>control</i> >	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 2 (config-terminal:2) level commands	
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".

echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 3 (config-terminal:3) level command	ls
break duration < milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.

exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <i><control></control></i>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 4 (config-terminal:4) level com	mands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.

login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 5 (config-terminal:5) level commands	
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current

settings.

Sets the optional send break character. <text> = the character. The character may be input as text,

send break <control>

	control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

terminal 6 (config-terminal:6) level con	nmands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.

terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 7 (config-terminal:7) level commands	
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

terminal 8 (config-terminal:8) level commands

break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 9 (config-terminal:9) level commands	
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".

echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 10 (config-terminal:10) level co	mmands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
1	I—

Exits to the configuration level.

On the login connect menu, removes the menu item allowing the user to exit to the CLI.

exit

exit connect menu disable

exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break < <i>control</i> >	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

terminal 11 (config-terminal:11) level c	commands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.

login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <i><control></control></i>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel < <i>line</i> >	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

	,
terminal 12 (config-terminal:12) level command	S
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text,</text>

	control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

terminal 13 (config-terminal:13) level commands	
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.

terminal network terminal type <text></text>	Enters the configure-terminal level for the network. Sets the terminal type.
tunnel	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 14 (config-terminal:14) level c	ommands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

terminal 15 (config-terminal:15) level commands

break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <control></control>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 16 (config-terminal:16) level co	mmands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".

echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break < <i>control</i> >	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal network (config-terminal:netw	ork) level commands
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".

echo disable

echo enable

exit connect menu disable

exit

Disables echoing of characters received on the line

Enables echoing of characters received on the line

On the login connect menu, removes the menu item

back to the line.

back to the line.

Exits to the configuration level.

allowing the user to exit to the CLI.

exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line	Enters the line level. line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <i><control></control></i>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.</control></text>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel < <i>line</i> >	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
traps (config-snmp-traps) level comma	nds
authentication password <text></text>	Sets password used for authentication for traps.
authentication protocol md5	Uses MD5 for authentication for traps.
authentication protocol sha	Uses SHA for authentication for traps.
clrscrn	Clears the screen.
community <text></text>	Sets the SNMP trap community string. <text> = name of the trap community string to be set.</text>
default authentication protocol	Restores to default SNMPv3 authentication method: MD5 for traps.
default community	Restores the SNMP trap community to default: public
default privacy protocol	Restores to default SNMPv3 privacy encryption method: DES for traps.
default security	Restores to default SNMPv3 security method: Authentication, No Privacy for traps.
default version	Restores to default SNMP version v2c for traps.
exit	Exits to the next higher level.
no authentication password	Clears authentication password for traps.
no primary destination	Deletes the primary SNMP trap host.
no privacy password	Clears privacy password for traps.
no secondary destination	Deletes the secondary SNMP trap host.
no username	Clears SNMPv3 username for traps.

primary destination <text></text>	Sets the primary SNMP trap host. <text> = IP address or hostname of SNMP trap receiver.</text>
privacy password <text></text>	Sets password used for privacy encryption for traps
privacy protocol aes	Uses AES for privacy encryption for traps.
privacy protocol des	Uses DES for privacy encryption for traps.
secondary destination <text></text>	Sets the secondary SNMP trap host. <text> = IP address or hostname of SNMP trap receiver.</text>
security authentication and privacy	Authentication and Privacy for traps.
security authentication but no privacy	Authentication, No Privacy for traps.
security no authentication and no priv	No Authentication, No Privacy for traps.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <text></text>	Sets SNMPv3 username for traps.
version snmpv1	Uses SNMPv1 for traps.
version snmpv2c	Uses SNMPv2c for traps.
version snmpv3	Uses SNMPv3 for traps.
write	Stores the current configuration in permanent memory.
trusted authorities (ssl-auth) level comma	nds
add	Adds an Authority Certificate.
clrscrn	Clears the screen.
delete all	Removes All Authority Certificates.
exit	Exits to the ssl level.
no intermediate authority < <i>cert</i> >	Removes an Intermediate Authority Certificate. <cert> = index displayed by "show authority" command.</cert>
no trusted authority <cert></cert>	Removes a Trusted Authority Certificate. <cert> = index displayed by "show authority" command.</cert>
show	Displays Authority Certificate Information.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
tunnel 1 (tunnel:1) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.

line < line>

no clear counters

modem

packing

serial

Enters the line level. line> = number of the line

(serial port) to be configured.

Unzeros all tunnel counters

Enters the modem level for this tunnel.

Enters the packing level for this tunnel.

Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 2 (tunnel:2) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 3 (tunnel:3) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 4 (tunnel:4) level commands		
accept	Enters the accept level for this tunnel.	
auto show statistics	show connection statistics	
clear counters	Zeros all tunnel counters	
clrscrn	Clears the screen.	
connect	Enters the connect level for this tunnel.	
disconnect	Enters the disconnect level for this tunnel.	
exit	Exits to the enable level.	
line	Enters the line level. line> = number of the line (serial port) to be configured.	
modem	Enters the modem level for this tunnel.	
no clear counters	Unzeros all tunnel counters	
packing	Enters the packing level for this tunnel.	
serial	Enters the serial level for this tunnel.	
show history	Displays the last 20 commands entered during the current CLI session.	
show statistics	show connection statistics	
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.	
terminal network	Enters the configure-terminal level for the network.	
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.	
write	Stores the current configuration in permanent memory.	

tunnel 5 (tunnel:5) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 6 (tunnel:6) level commands		
accept	Enters the accept level for this tunnel.	
auto show statistics	show connection statistics	
clear counters	Zeros all tunnel counters	
clrscrn	Clears the screen.	
connect	Enters the connect level for this tunnel.	
disconnect	Enters the disconnect level for this tunnel.	
exit	Exits to the enable level.	
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.	
modem	Enters the modem level for this tunnel.	
no clear counters	Unzeros all tunnel counters	
packing	Enters the packing level for this tunnel.	
serial	Enters the serial level for this tunnel.	
show history	Displays the last 20 commands entered during the current CLI session.	
show statistics	show connection statistics	
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.	
terminal network	Enters the configure-terminal level for the network.	
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.	
write	Stores the current configuration in permanent memory.	

tunnel 7 (tunnel:7) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 8 (tunnel:8) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 9 (tunnel:9) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 10 (tunnel:10) level commands		
accept	Enters the accept level for this tunnel.	
auto show statistics	show connection statistics	
clear counters	Zeros all tunnel counters	
clrscrn	Clears the screen.	
connect	Enters the connect level for this tunnel.	
disconnect	Enters the disconnect level for this tunnel.	
exit	Exits to the enable level.	
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.	
modem	Enters the modem level for this tunnel.	
no clear counters	Unzeros all tunnel counters	
packing	Enters the packing level for this tunnel.	
serial	Enters the serial level for this tunnel.	
show history	Displays the last 20 commands entered during the current CLI session.	
show statistics	show connection statistics	
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.	
terminal network	Enters the configure-terminal level for the network.	
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.	
write	Stores the current configuration in permanent memory.	

tunnel 11 (tunnel:11) level command	S
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. < = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 12 (tunnel:12) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 13 (tunnel:13) level command	s
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel < line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 14 (tunnel:14) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 15 (tunnel:15) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. <pre></pre><pre>configure</pre><pre>terminal line (serial port) to be configured.</pre>
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

tunnel 16 (tunnel:16) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line <line></line>	Enters the line level. line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal <line></line>	Enters the configure-terminal level. line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.

xml (xml) level commands	
clrscrn	Clears the screen.
exit	Exits to the enable level.
secret xcr dump	Dump XML configuration containing secrets to the console
secret xcr dump < group list>	Dump specified XML configuration containing secrets to the console
secret xcr export <file></file>	Save XML configuration containing secrets to a file
secret xcr export <file> <group list=""></group></file>	Save specified XML configuration containing secrets to a local file
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
xcr dump	Dump XML configuration to the console

xcr dump < <i>group list</i> >	Dump specified XML configuration to the console
xcr export <file></file>	Save XML configuration to a file
xcr export <file> <group list=""></group></file>	Save specified XML configuration to a local file
xcr import <file></file>	Load XML configuration from a local file
xcr import <file> <group list=""></group></file>	Load specified XML configuration from a local file
xcr list	List XML Configuration Record groups to the console
xsr dump	Dump XML Status Records to the console
xsr dump < <i>group list</i> >	Dump specified XML Status Records to the console
xsr export <file></file>	Save XML Status Record to a file
xsr export <file> <group list=""></group></file>	Save specified XML Status Record to a local file
xsr list	List XML Status Record groups to the console