



# **EDS-**MD<sup>®</sup> **Medical Device Server Command Reference**

◆EDS-MD 4

**◆EDS-MD** 8

**◆EDS-MD 16** 

## **Intellectual Property**

© 2015 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* and *EDS-MD* are registered trademarks of Lantronix, Inc. in the United States and other countries. *DeviceInstaller* is a trademark of Lantronix, Inc. U.S. Patents 7,698,405; 8,024,446; 8,219,661; 8,504,740. 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. Corporate Headquarters

167 Technology Drive Irvine, CA 92618, USA Toll Free: 800-526-8766 Phone: 949-453-3990 Fax: 949-453-3995

**Technical Support** 

Online: www.lantronix.com/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/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.

## **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.	

# **Table of Contents**

Intellectual Property	
Contacts	
Disclaimer	
Revision History	
List of Figures	
List of Tables	!
1: About This Guide	
Chapter Summaries	(
Conventions	
Additional Documentation	
2: Overview	8
XML Architecture and Device Control	1
Command Line Interface	
3: Command Line Interface	Ş
Configuration Using Telnet	,
Configuration Using Serial Lines	
Boot to CLI and Device Recovery	
Navigating the CLI Hierarchy	
Using Keyboard Shortcuts and CLI	1
Understanding the CLI Level Hierarchy	1
4: Configuration Using XML	14
XML Configuration Record Document Type Definition	1
Quick Tour of XML Syntax	
Declaration	1
Element Start and End Tags	1
Element Attributes	1
Record, Group, Item, and Value Tags	10
Importing and Exporting an XML Configuration File	18
Best Practices	
Importing	
Exporting	
XML Configuration Groups	
XML Status Record Groups and Items	29
5: Commands and Levels	38

# **List of Figures**

Figure 3-2 CLI Level Hierarchy	12
Figure 3-3 Login Level Commands	12
Figure 3-4 Enable Level Commands	13
Figure 4-1 DTD for XCRs	14
Figure 4-2 XML Example	15
Figure 4-3 XML Example	16
Figure 4-4 XML Example of Multiple Named Values	16
Figure 4-5 XML Example of Multiple Items	17
Figure 4-6 XML Example with Multiple Groups	17

# **List of Tables**

Table 3-1 Keyboard Shortcuts	11
Table 4-7 XCR Groups	20
Table 4-8 XSR Group and Items	29
Table 5-1 Commands and Levels	47

# 1: About This Guide

This guide describes how to configure the Lantronix® EDS-MD® medical device server 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 device servers (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 medical device servers.
Chapter 4: Configuration Using XML	Lists XCR groups and items and describes how to use XCRs to configure the EDS-MD 4/8/16 medical device servers.
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	<b>Note:</b> Means take notice. Notes contain helpful suggestions, informatio 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 <a href="www.lantronix.com/support/documentation">www.lantronix.com/support/documentation</a> for the latest documentation and the following additional documentation.

Document	Description
EDS-MD Medical Device Server User Guide	Describes how to configure and use an EDS-MD 4/8/16 medical device server.
Com Port Redirector Quick Start and Online Help	Instructions for using the Lantronix Windows based utility to create virtual com ports.
DeviceInstaller Online Help	Instructions for using the Lantronix Windows based utility to locate an EDS-MD 4/8/16 medical device server and to view its current settings.

# 2: Overview

The EDS-MD 4, EDS-MD 8 and EDS-MD 16 medical device servers 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 Medical Device Server 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 device server supports XML configuration records that make configuring the device server 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**

Making the edge-to-enterprise vision a reality, the EDS-MD 4/8/16 device server uses industry-standard tools for configuration, communication, and control. For example, the EDS-MD 4/8/16 device 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 medical device server.

# 3: Command Line Interface

This chapter describes accessing the EDS-MD 4, EDS-MD 8 or EDS-MD 16 medical device server 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 medical device server 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 <a href="www.lantronix.com/support/downloads">www.lantronix.com/support/downloads</a>.

To access the EDS-MD 4/8/16 device server 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 is the IP address) in a Windows/Linux command prompt.
- 4. The EDS-MD 4/8/16 device 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 Medical Device Server 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 Lantronix device serverlocally using a serial port:

- 1. Connect a terminal or a PC running a terminal emulation program to one of the device server'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 medical device server 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 device server using the CLI:

<b>Key Combination</b>	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

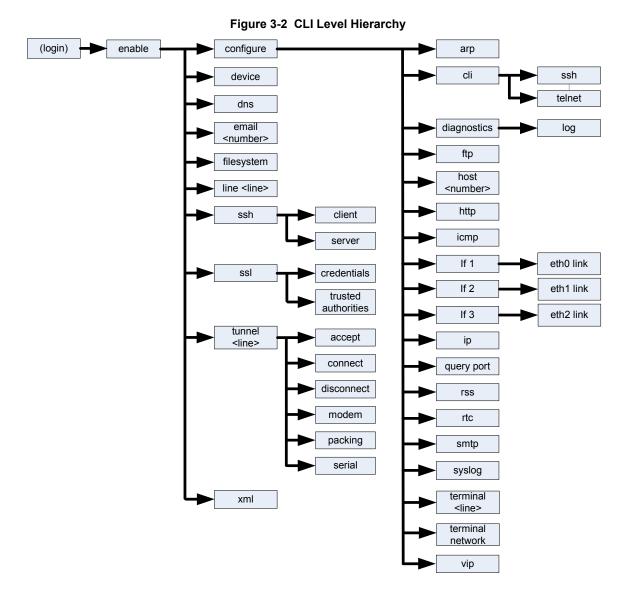
# **Understanding the CLI Level Hierarchy**

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 medical device server. 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.

An overview of the levels in the EDS-MD 4/8/16 device server 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 device server, 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
kill ssh <session>
                                                                     kill telnet <session>
line <line>
                                                                     ping <host>
ping <host> <count>
                                                                     ping <host> <count> <timeout>
reload
                                                                     reload factory defaults
show
                                                                     show history
show interfaces
                                                                     show ip sockets
show lines
                                                                     show processes
show sessions
ssh <optClientUsername> <host>
                                                                     ssh <optClientUsername> <host> <port>
                                                                     telnet <host>
telnet <host> <port>
                                                                     trace route <host>
                                                                     tunnel <line>
trace route <host>                                                                                                                                                                                                                                                                                                                                                  
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 medical device server provides an Extensible Markup Language (XML) interface that you can use to configure device server devices. Every configuration setting that can be issued from the device server Web Manager and CLI can be specified using XML.

The device server 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 medical device server 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 device server, 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 medical device servers.

# 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 medical device server 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 Medical Device Server 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 device 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 device server file system and imported or accessed as needed. See <u>Best Practices on page 18</u> or the Filesystem Browser section in the <u>EDS-MD</u> <u>Medical Device Server User Guide</u>.
- 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 device server 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 device server file system. It can also be used to import an XCR from an external source such as your local hard drive.
- FTP-The device server 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 device 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 device server 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 Medical Device Server 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 device server. 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 device server 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 device server 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 device server 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 device server 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 device server 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 to 12.xcr on the device serverfilesystem.

```
xcr export tunnel config t1 l2.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 device server filesystem:

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

# **XML Configuration Groups**

*Table 4-7* lists the EDS-MD 4/8/16 device server 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 **&#60** in the table may be read as "less than" and any instance of **&#62** may be read as "greater than".

Table 4-7 XCR Groups

<b>Group Name</b>	Group Item	Value Name	Value Options	Additional Information
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	time set	day of month		
		month		
		hours		
		minutes		
		seconds		
		year		
	time zone	offset		
		zone		
device	firmware version			Read only.
	long name			
	serial number			Read only.
	short name			
diagnostics	log	output		
		max length		

<b>Group Name</b>	Group Item	Value Name	<b>Value Options</b>	Additional
(continued)	·			Information
email ("Instance" attribute is a number.)	СС			
	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
attribute is "eth0", "eth1", or "eth2".)	speed		auto, 10, 100	Default: auto
ftp server	state		enable, disable	Default: enable
host	name			
("Instance" attribute is a number.)	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	
interface	bootp		enable, disable	Default: disable
("Instance" attribute	dhcp		enable, disable	Default: enable
is "eth0", "eth1", or "eth2")	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

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
line	name			
("Instance" attribute is a number.)	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
	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
query port	state		enable, disable	Default, enable
rss	feed		enable, disable	Default: disable
	persist		enable, disable	Default: disable
	max entries			Default: 100
serial command mode ("Instance"	mode		always, serial string, disable	Default: disable
attribute is a	echo serial string		enable, disable	Default: enable
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.

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
serial command mode ("Instance" attribute is a number.) (continued)	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
ssh	state		enable, disable	Default: enable
	port			Default: 22
	max sessions			Default: 3
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		

Group Name (continued)	<b>Group Item</b>	Value Name	Value Options	Additional Information
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		
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

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
terminal	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
tunnel accept	accept mode		disable, always	Default: always
("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" 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 number)	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" 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	echo pluses		enable, disable	Default: disable
("Instance" attribute	echo commands		enable, disable	Default: enable
is a number.)	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" attribute	packing mode		disable, timeout, send character	Default: disable
is a number.)	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" 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

<b>Group Name</b>	Item Name	Value Name	Valid Values
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	
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" attribute	success	sent	decimal number
is " <decimal>")</decimal>		sent with retries	decimal number
	failed		decimal number
	queued		decimal number
email log ("Instance" attribute is " <decimal>")</decimal>	entry	time	timestamp in format d days hh:mm:ss
		log	string
hardware	сри	speed	string
		type	string
	memory	flash size	decimal number
		ram size	decimal number
http	state		
	logging	entries	
		bytes	

<b>Group Name (continued)</b>	Item Name	Value Name	Valid Values
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

<b>Group Name (continued)</b>	Item Name	Value Name	Valid Values
interface ("Instance"	default gateway	status	dotted notation
attribute is "eth0", "eth1",	ip address		dotted notation
or "eth2")	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

<b>Group Name (continued)</b>	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" attribute is	receiver	bytes	decimal number
" <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
		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

<b>Group Name (continued)</b>	Item Name	Value Name	Valid Values
line (group nested within	state		enable or disable
line above)	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&#62 ;Q</control&#62 
	xoff char		of form <control&#62 ;S</control&#62 
memory	main heap	total memory	decimal number of bytes
processes	process ("Instance" attribute is " <decimal>")</decimal>	stack used	decimal number
		stack size	decimal number
		cpu %	decimal number
		thread name	String
query port	last connection	ip address	ip address in format 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	
rss	url		string in the form of a web url
	data	entries	decimal number
		bytes	decimal number
sessions	telnet or ssh ("Instance"	local port	
	attribute is " <number>")</number>	remote ip address	
		remote port	
		duration	

<b>Group Name (continued)</b>	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
		OutOfWindowlcmps	decimal number
		LockDroppedIcmps	decimal number
		ArpFilter	decimal number
		TW	decimal number
		TWRecycled	decimal number
		TWKilled	decimal number
	F	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

<b>Group Name (continued)</b>	Item Name	Value Name	Valid Values
tcp (continued)	netstat (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

<b>Group Name (continued)</b>	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" 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

<b>Group Name (continued)</b>	Item Name	Value Name	Valid Values
tunnel ("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	echo commands	enable, disable	
	verbose response	enable, disable	
	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

- enable (enable)
  - configure (config)
    - arp (config-arp)
    - cli (config-cli)
      - ssh (config-cli-ssh)
      - telnet (config-cli-telnet)
      - diagnostics (config-diagnostics)
        - log (config-diagnostics-log)
    - ftp (config-ftp)
    - 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)
    - 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)
- <u>query port (config-query port)</u>
- rss (config-rss)
- rtc (config-rtc)
- smtp (config-smtp)
- 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 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)
- terminal network (config-terminal:network)
- vip (config-vip)
- device (device)
- dns (dns)
- email 1 (email:1)
- email 2 (email:2)
- email 3 (email:3)
- <u>email 4 (email:4)</u>
- 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)
- - il 40 (- - il 40)
- 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 o (turnel-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 10 (turnel-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 14 (turnel-connect-host:6:15)
    - ilost 15 (turiner-connect-riost.o. 15)
    - host 16 (tunnel-connect-host:6:16)
  - <u>disconnect (tunnel-disconnect:6)</u>modem (tunnel-modem:6)
  - packing (tunnel-packing:6)
  - backing (tarifici packing
  - 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)
- <u>disconnect (tunnel-disconnect:9)</u>
- 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 & (turiner-connect-nost, 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)
- <u>tunnel 11 (tunnel:11)</u>
  - 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)
- <u>disconnect (tunnel-disconnect:11)</u>
- 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 46 (tunnel-connect-host:44:46)
    - 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)

Table 5-1 Commands and Levels

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 punc-

	tuation: 123ABC "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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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
<del></del>	

	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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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

accept mode modem emulation  Enables accept mode unneling when the configured start character  Enables accept mode unneling when the configured start character is received on the line.  Sets the accept unnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC '12,3A, BC 12,3A, BC 12,3a, bc 12,3a bc		control pin is asserted.
character is received on the line.  aes decrypt key <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 112 3A BC 112 3</hexadecimal>	accept mode modem emulation	Enables modem emulation for accept mode tunneling.
bytes. 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 ABC 12.3 a.bc 12.3 a.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.  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.  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 *12.3 ABC *12.3 ABC *12.3 a.bc *12.3 a.bc Note that quotes must enclose the value if it contains spaces.  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.  Biock network disable  Forwards (tunnels) network data in accept mode tunneling.  Biock network enable  Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).  Biock 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.  Credentials <fext> Selects the RSA/DSA certificates by name for the SSL server.  Gelault local port  Uses the default port number as the local port for accept mode tunneling.  Uses the default port number as the local port for accept mode tunneling.  Uses the default port number as the local port for accept mode tunneling.  Bestores the default port number as the local port for accept mode tunneling.  Uses the default port tool as *TCP*.  Gefault teacept mode start character.  default top keep alive  Restores the default port ouse to send an email alert upon</fext>	accept mode start character	character
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 12,3a;bc Note that quotes must enclose the value if it contains spaces.  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.  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).  Cirscm Clears the screen.  Clears the screen.  Credentials <text> 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 number as the local port for accept mode default port number as the local port for accept mode tunneling. The default port number as the local port for accept mode tunneling. The default port number as the local port for accept mode default port number as the local port for accept mode tunneling. 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 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 port cool as "TCP".  Defaults the accept mode start character.  Restores the default port soul accept mode TCP keep alive timeout.</text></hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by 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 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 disable Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).  clrscrn Clears the accept mode tunnel (generally used for debugging).  clrscrn Clears the screen.  credentials <text> Selects the RSA/DSA certificates by name for the SSL server.  default accept mode Restores the default accept mode as "always".  Uses 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 torotocol Restores the default protocol as "TCP".  default top alive timeout.  email connect <number> Sets an email profile to use to send an email alert upon</number></text>	aes decrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
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).  Clears the accept mode tunnel (generally used for debugging).  Clears the screen.  Credentials <text>  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 start character  Defaults the accept mode start character.  default top keep alive  Restores the default protocol as "TCP".  Sets an email profile to use to send an email alert upon</text>	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
block network enable  block network enable  block network enable  block serial disable  block serial disable  block serial disable  block serial enable  block serial 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>  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 start character  befaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  email connect <number>  Sets an email profile to use to send an email alert upon</number></text>	aes encrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
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).  Clears the screen.  Clears the screen.  Credentials < text> 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 start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.	block network disable	
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> 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 start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  Sets an email profile to use to send an email alert upon</text>	block network enable	before forwarding
forwarding it to the accept mode tunnel (generally used for debugging).  clrscrn  Clears the screen.  credentials <text>  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 start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  Sets an email profile to use to send an email alert upon</text>	block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
credentials <text>  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 start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  email connect <number>  Sets an email profile to use to send an email alert upon</number></text>	block serial enable	it to the accept mode tunnel (generally used for debug-
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 start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  Sets an email profile to use to send an email alert upon	clrscrn	Clears the screen.
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 start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  email connect <number>  Sets an email profile to use to send an email alert upon</number>	credentials <text></text>	
mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.  default protocol Restores the default protocol as "TCP".  default start character Defaults the accept mode start character.  default tcp keep alive Restores the default 45 second accept mode TCP keep alive timeout.  email connect <number> Sets an email profile to use to send an email alert upon</number>	default accept mode	Restores the default accept mode as "always".
default start character  Defaults the accept mode start character.  default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  email connect <number>  Sets an email profile to use to send an email alert upon</number>	default local port	mode tunneling. The default port is 10000 + #, where # is the line number
default tcp keep alive  Restores the default 45 second accept mode TCP keep alive timeout.  email connect <number>  Sets an email profile to use to send an email alert upon</number>	default protocol	Restores the default protocol as "TCP".
alive timeout.  email connect <number>  Sets an email profile to use to send an email alert upon</number>	default start character	Defaults the accept mode start character.
	default tcp keep alive	
	email connect <number></number>	

	an accept mode tunnel.
email disconnect < number>	<pre><number> = the number of the email profile to use.</number></pre> Sets an email profile to use to send an email alert upon
email disconnect < number >	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
ilusii seriai disable	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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:14) 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".

	1
	mode tunneling.  The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <pre>control &gt; C. A decimal value character has the form \( \) 99. A hex value character has the form \( \) 99. A hex value character has the form \( \) 99. A hex value character has the form \( \) 99. Enables TCP keep alive for accept mode tunneling and sets the timer. <pre>crition of the value in milliseconds.</pre>  ### To Pkeep alive for accept mode tunneling and sets the timer.  ### To Pkeep alive for accept mode tunneling and sets the timer.  ### To Pkeep alive for accept mode tunneling and sets the timer.  ### To Pkeep alive for accept mode tunneling and sets the timer.  ### To Pkeep alive for accept mode tunneling and sets the tunneling server to always accept tunneling connections.  ### To Pkeep alive for accept tunneling connections.  ### To Pkeep alive for accept tunneling connections.  ### To Pkeep alive for accept tunneling connections only when a character is received through the corresponding line (serial port).  ### To Pkeep alive for accept tunneling connections only when a character is received mode tunneling.  ### To Pkeep alive for accept tunneling connections only when a character is received mode tunneling.  ### Accept mode modem control asserted  ### Enables accept mode tunneling server to accept tunneling connections when the modem control pin is asserted.  ### Accept mode modem emulation  ### Accept mode modem emulation  ### Accept mode 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 the digits.  ### Bytes may run together or be separated by optional punctuation.  ### 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.  ### Bytes may run together or be separated by optional punctuation.  ### Accept tunnel AES encrypt key with up to 16</pre>		
sels the timer.  "chilliseconds> = timer value, in milliseconds.  write  Stores the current configuration in permanent memory.  Eccept (funnel-accept-13) level commands  accept mode always  Enables the tunneling server to always accept tunneling connections.  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).  accept mode disable  Disables accept mode tunneling.  Enables the tunneling server to accept tunneling connections when the modern control pin is asserted.  Enables mode menulation of accept mode tunneling, enables accept mode tunneling when the configured start character  Enables accept mode tunneling when the configured start character is received on the line.  Best 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.  Best the accept tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by a wingle character.  Note that quotes must enclose the value if it contains spaces.  Best 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 *123ABC* *123AB		A decimal value character has the form \99.
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).  Disables accept mode tunneling.  accept mode modem control asserted  Enables the tunneling server to accept tunneling connections when the modem control asserted.  Enables accept mode tunneling.  Enables accept mode unneling when the configured start character  Enables accept mode unneling when the configured start character is received on the line.  Best 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  Note that quotes must enclose the value if it contains spaces.  Best character tunnel AES decrypt key with up to 16 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.  Best 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  Note that quotes must enclose the value if it contains spaces.  Best 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  Note that quotes must enclose the value if it contains spaces.  Best 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 tun	tcp keep alive <milliseconds></milliseconds>	sets the timer.
accept mode always  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).  accept mode disable  Disables accept mode tunneling.  accept mode modern control asserted  Enables the tunneling server to accept tunneling connections when the modern control price is asserted.  Enables modern emulation for accept mode tunneling.  accept mode start character  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 12.3a bc 12.3a bc Note that quotes must enclose the value if it contains spaces.  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.  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	write	Stores the current configuration in permanent memory.
accept mode always  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).  accept mode disable  Disables accept mode tunneling.  accept mode modern control asserted  Enables the tunneling server to accept tunneling connections when the modern control price is asserted.  Enables modern emulation for accept mode tunneling.  accept mode start character  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 12.3a bc 12.3a bc Note that quotes must enclose the value if it contains spaces.  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.  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	accept (tunnel-accept:13) level commands	
tions only when a character is received through the corresponding line (serial port).  accept mode disable  Disables accept mode tunneling.  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.  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.  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.  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,b		
Enables the tunneling server to accept tunneling connections when the modern control pin is asserted.  accept mode modern emulation  Enables modern emulation for accept mode tunneling.  Enables accept mode tunneling when the configured start character  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.  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.  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.  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.  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.  Diock network disable  Forwards (tunnels) network data in accept mode tunnel before forwarding it to the serial interface (generally used for debugging).	accept mode any character	tions only when a character is received through the corresponding line (seri-
tions when the modem control pin is asserted.  accept mode modem emulation  Enables modem emulation for accept mode tunneling.  Enables accept mode tunneling when the configured start character is received on the line.  aes decrypt key <*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.  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 Note that quotes must enclose the value if it contains spaces.  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 Note that quotes must enclose the value if it contains spaces.  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 tunnel before forwarding it to the serial interface (generally used for debugging).	accept mode disable	Disables accept mode tunneling.
accept mode start character  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.  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.  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.  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 tunnel-ling.  Discards all data coming in from the accept mode tunnel-before forwarding it to the serial interface (generally used for debugging).	accept mode modem control asserted	tions when the modem
character is received on the line.  aes decrypt key <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.  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.  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.  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.  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.  Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).</hexadecimal>	accept mode modem emulation	Enables modem emulation for accept mode tunneling.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  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.  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.  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.  Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).</text>	accept mode start character	character
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  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.  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).	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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).</text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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).	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
block network enable  Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).	aes encrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
before forwarding it to the serial interface (generally used for debugging).	block network disable	1
block serial disable Forwards (tunnels) serial data in accept mode tunneling.	block network enable	before forwarding
	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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
	I
protocol tcp	Uses TCP protocol for accept mode tunneling.

	tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
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 >	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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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.
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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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
accept filoue always	connections.
accept mode always accept mode any character	
·	connections.  Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (seri-
accept mode any character	connections.  Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode any character accept mode disable	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
accept mode any character  accept mode disable accept mode modem control asserted	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.
accept mode any character  accept mode disable accept mode modem control asserted  accept mode modem emulation	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

aes encrypt key <hexadecimal> aes encrypt key text <text></text></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.  Sets the accept tunnel AES encrypt key with up to 16
acs charget key text stexts	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).
cirscrn	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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.

kill connection	Disconnects the active accept mode tunneling connection.
local port <number></number>	Sets the port to use for accept mode tunneling.
local port	<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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:10) 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 punc-
	tuation:
	123ABC "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
aces cherypt key shexadeoimar	bytes.
	Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:
	123ABC "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
black assist disciple	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 debug-
	ging).
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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep
· ·	alive timeout.
email connect <number></number>	Sets an email profile to use to send an email alert upon
	establishing an accept mode tunnel.
	<pre><number> = the number of the email profile to use.</number></pre>
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
Indon donal disable	Characters alleady in the serial data buller are retailled

	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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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	

	tions 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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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
email disconnect (number)	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
iliusii seriai disable	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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
<u> </u>	

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 <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 < <i>text</i> >	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 <i><hexadecimal></hexadecimal></i>	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 start character	Defaults the accept mode start character.
default top keep alive	Restores the default 45 second accept mode TCP keep
· ·	alive timeout.
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.
kill connection	Disconnects the active accept mode tunneling connection.
local port < <i>number</i> >	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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 aes encrypt key no credentials	Removes the accept tunnel AES encrypt key. Clears the RSA/DSA certificate selection.

	accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept
	mode tunnel.
no tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
write accept (tunnel-accept:5) level commands	Stores the current configuration in permanent memory.
	Stores the current configuration in permanent memory.  Enables the tunneling server to always accept tunneling connections.
accept (tunnel-accept:5) level commands	Enables the tunneling server to always accept tunneling
accept (tunnel-accept:5) level commands accept mode always	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 (seri-
accept (tunnel-accept:5) level commands accept mode always accept mode any character	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).
accept (tunnel-accept:5) level commands accept mode always accept mode any character accept mode disable	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
accept (tunnel-accept:5) level commands accept mode always accept mode any character accept mode disable accept mode modem control asserted	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.
accept (tunnel-accept:5) level commands accept mode always accept mode any character accept mode disable accept mode modem control asserted accept mode modem emulation	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

	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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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></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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:3) 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 <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 <i><hexadecimal></hexadecimal></i>	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 < <i>text</i> >	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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.

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>	·
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.

accept (tunnel-accept:2) 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 <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 < <i>text</i> >	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 <i><hexadecimal></hexadecimal></i>	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 start character	Defaults the accept mode start character.
default top keep alive	Restores the default 45 second accept mode TCP keep
· ·	alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
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></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 start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
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.
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 tcp keep alive	Disables the accept mode TCP keep alive timeout.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory.
arp (config-arp) level commands	
add <ip address=""> <mac address=""></mac></ip>	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 address in colon-separated form.</mac></ip>
clrscrn	Clears the screen.
exit	Exits to the configuration level.
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 used to quit the "connect line <li><li>command.</li></li>
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 <li>command.  The characters may be input as text or control.  A control character has the form <control>C.</control></li>

Displays the current configuration.
Displays the last 20 commands entered during the current
CLI session.
Change to menu level for SSH configuration and status.
Change to menu level for Telnet configuration and status.
Stores the current configuration in permanent memory.
Clears the screen.
Restore the user command to the default login shell
Remove all hnown hosts
Remove all users
Remove known host
Delete the named user
Exits to the ssh level.
Set known host RSA or DSA key
Remove known host DSA key
Remove known host RSA key
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.
Changes to the command level for ARP configuration and status.
Change to menu level for CLI configuration and status
Clears the screen.
Enters the diagnostics level.
Exits to the enable level.
Enters the ftp level.
Change to config host level
Enters the http level.
Enters the http level.

I .	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"
query port	Enters the query port level.
rss	Change to menu level for RSS configuration and status
rtc	Change to menu level for Real Time Clock 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.
syslog	Enters the syslog level.
terminal <line></line>	Enters the configure-terminal level. <pre><li><li><ne>&lt; = number of the terminal line (serial port) to be configured.</ne></li></li></pre>
terminal network	Enters the configure-terminal level for the network.
vip	Change to menu level for VIP configuration and status
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:16) level commands	
block network disable	Famus and a (tripped a) in attribute in a supper transfer tripped
	Forwards (tunnels) network data in connect mode tunneling.
block network enable	I.
	ing.  Discards all data coming in from the connect mode tunnel before forwarding
block network enable	ing.  Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block network enable block serial disable	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debug-
block network enable block serial disable block serial enable	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.
block network enable block serial disable block serial enable clrscrn	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling
block network enable block serial disable block serial enable clrscrn connect mode always	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial
block network enable  block serial disable  block serial enable  clrscrn  connect mode always  connect mode any character	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
block network enable  block serial disable  block serial enable  clrscrn  connect mode always  connect mode any character  connect mode disable	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).  Disables connect mode tunneling.  Enables the tunneling server to make tunneling connections when the modem
block serial disable block serial enable  clrscrn connect mode always  connect mode any character  connect mode disable connect mode modem control asserted	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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).  Disables connect mode tunneling.  Enables the tunneling server to make tunneling connections when the modem control pin is asserted.

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.</control>
	A decimal value character has the form \99.
	A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:15) 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></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).
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.

nection when a character is received on the corresponding line (serial port).  connect mode disable  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 connect mode muneling when the configured start character  Enables connect mode tunneling when the configured start character size received on the line.  Restores the default connect mode as "disable".  Connects to the first host in the list that accepts the connections to other devices.  default local port  Uses a random port number as the local port for establishing unnelling connect mode tunneling.  Connects to other devices.  default reconnect time  Restores the default reconnect time value for connect mode tunneling.  Connect so other devices.  Restores the default reconnect time value for connect mode tunneling.  Connect on the devices.  Restores the default reconnect make a mail alert upon establishing a connect mode start character.  Defaults the connect mode start character.  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.  -numbers = 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 a connect mode tunnel.  Flush serial disable  Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer pronestablishing a connect mode tunneling connection.  Enables forwarding of the connect start character into the network.  Disables forwarding of the connect start character into the network.  Disables for first host in the list that accepts the connection.  Enters the next lower level.  Selects simultaneous connections to all hosts on the host list.  Selects simultaneous connections to all hosts on the host list.  Connects to the fir		
Enables the tunneling server to make tunneling connections when the modern control pin is asserted.  connect mode modem emulation  Enables modem emulation for connect mode tunneling.  Enables connect mode tunneling when the configured start character serviced on the line.  default connect mode  Restores the default connect mode as "disable",  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 reconnect time  Restores the default reconnect time value for connect mode tunneling.  default start character  Defaults the connect mode start character.  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.  **crumber>**  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.  **crumber> 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 a connect mode tunneling.  flush serial enable  Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  flush start character enable  Disables forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect start character into the network.  Possibles forwarding of the connect sta	connect mode any character	nection when a character is received on the corresponding line (serial
tions when the modem control pin is asserted.  Connect mode modem emulation Connect mode start character  Enables connect mode tunneling when the configured start character start character is received on the line.  Restores the default connect mode as "disable".  default host mode  Connects to the first host in the list that accepts the connection.  Uses a random port number as the local port for establishing tunneling connections to other devices.  Restores the default reconnect time value for connect mode tunneling.  default start character  Defaults the connect mode start character.  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.  exit  Returns to the tunnel level.  Characters already in the serial data buffer are retained upon establishing a connect mode tunnelling.  flush serial enable  Characters already in the serial data buffer are retained upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the serial data buffer upon establishing a connect mode tunnelling connection.  Flushes the first host in the list that accepts the connect since the first host in the list that accepts the connect mode simultaneous  Selects simultaneous connections to all hosts on the host list.  kill connects the first host in the list that accepts the connection or connections.  Sets a specific port for use as the lo	connect mode disable	Disables connect mode tunneling.
Enables 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".  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.  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.  Restores the default reconnect time value for connect mode tunnel.  **email connect **number**  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.  **email disconnect **number**  Sets an email profile to use to send an email alert upon closing a connect mode tunnel.  **email profile to use to send an email profile to use.  Returns to the tunnel level.  Returns to the tunnel level.  Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  If ush serial enable  Gharacters already in the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Connects to the instance for the connect start character into the network.  Place the serial data buffer upon establishing a connect mode simultaneous  Sets a specific port for use as the local port.  **email profile to use to send an email alerts upon establishing a connect mode tunnel.  Connects to the first host in the	connect mode modem control asserted	tions when the modem
start character is received on the line.  default connect mode Restores the default connect mode as "disable".  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 trunneling 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.  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.	connect mode modem emulation	Enables modem emulation for connect mode tunneling.
default local port  default local port  Uses a random port number as the local port for establishing tunneling connections to other devices.  Restores the default reconnect time Restores the default reconnect time value for connect mode tunneling.  default start character  Defaults the connect mode start character.  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.  «number»  Email disconnect «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.  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.  Returns to the tunnel level.  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.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Enables forwarding of the connect start character into the network.  Flush start character enable  Disables forwarding of the connect start character into the network.  Enters the next lower level.  Specify the instance for the next lower level.  Selects simultaneous connections to all hosts on the host list.  Disconnects the active connect mode tunneling connection or connections.  Sets a specific port for use as the local port.  «number» = the number of the port to use.  Disconnect mode tunnel.	connect mode start character	start character
nection.	default connect mode	Restores the default connect mode as "disable".
ing tunneling connections to other devices.  default reconnect time  Restores the default reconnect time value for connect mode tunneling.  Defaults the connect mode start character.  Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> start email profile to use to send an email profile to use.  Sets an email profile to use to send an email profile to use.  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.  Exit  Returns to the tunnel level.  Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushs 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.  Enters the next lower level.  Specify the instance for the next lower level.  Connects to the first host in the list that accepts the connection.  bost mode sequential  Connects to the first host in the list that accepts the connection.  Selects simultaneous connections to all hosts on the host list.  kill connection  Disconnects the active connect mode tunneling connection or connections.  Sets a specific port for use as the local port.  <number> the number&gt; the number of the port to use.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number></number>	default host mode	
default start character  Defaults the connect mode start character.  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.  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.  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.  Returns to the tunnel level.  Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flush start character disable	default local port	
Sets an email profile to use to send an email alert upon establishing a connect mode tunnel.  email disconnect < number> Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. Sets an email profile to use to send an email alert upon closing a connect mode tunnel. exit Returns to the tunnel level. 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> Enters the next lower level. Specify the instance for the next lower level. Specify the instance for the next lower level. 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. Sets a specific port for use as the local port. cumber&gt; no email connect Discontinues sending email alerts upon establishing a connect mode tunnel.</instance>	default reconnect time	
establishing a connect mode tunnel. <number> = the number of the email profile to use.  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.  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.  exit  Returns to the tunnel level.  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.  Instance&gt;  Enters the next lower level. Specify the instance for the next lower level.  Specify the instance for the next lower level.  Connects to the first host in the list that accepts the connection.  bost mode simultaneous  Selects simultaneous connections to all hosts on the host list.  kill connection  Disconnects the active connect mode tunneling connection or connections.  Sets a specific port for use as the local port. <number> = the number of the port to use.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number></number></number>	default start character	Defaults the connect mode start character.
closing a connect mode tunnel. exit Returns to the tunnel level. Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  Flushes serial enable  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Enables forwarding of the connect start character into the network.  Disables forwarding of the connect start character into the network.  Enters the next lower level.  Specify the instance for the next lower level.  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.  Sets a specific port for use as the local port. <	email connect < <i>number</i> >	establishing a connect mode tunnel.
Returns to the tunnel level.  Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Enables forwarding of the connect start character into the network.  Disables forwarding of the connect start character into the network.  Enters the next lower level.  Specify the instance for the next lower level.  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.  Disconnects the active connect mode tunneling connection or connections.  Sets a specific port for use as the local port. <number>  Discontinues sending email alerts upon establishing a connect mode tunnel.</number>	email disconnect < number >	closing a connect mode tunnel.
upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Flushes the serial data buffer upon establishing a connect mode tunneling connection.  Enables forwarding of the connect start character into the network.  Disables forwarding of the connect start character into the network.  Enters the next lower level.  Specify the instance for the next lower level.  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.  Sets a specific port for use as the local port. <number> = the number of the port to use.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number>	exit	
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.  bost <instance>  Enters the next lower level. Specify the instance for the next lower level.  Connects to the first host in the list that accepts the connection.  bost 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.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number></instance>	flush serial disable	upon establishing
network.  Disables forwarding of the connect start character into the network.  host <instance>  Enters the next lower level. Specify the instance for the next lower level.  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.  Sets a specific port for use as the local port.  <number> = the number of the port to use.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></instance>	flush serial enable	
network.  Enters the next lower level. Specify the instance for the next lower level.  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.  Sets a specific port for use as the local port. <number> = the number of the port to use.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number>	flush start character disable	
Specify the instance for the next lower level.  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.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number>	flush start character enable	Disables forwarding of the connect start character into the network.
nection.  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.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number>	host <instance></instance>	
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.  Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number>	host mode sequential	·
tion or connections.    local port <number>   Sets a specific port for use as the local port. <number> = the number of the port to use.    Discontinues sending email alerts upon establishing a connect mode tunnel.</number></number>	host mode simultaneous	
<pre>cnumber&gt; = the number of the port to use.</pre> no email connect Discontinues sending email alerts upon establishing a connect mode tunnel.	kill connection	
connect mode tunnel.	local port <number></number>	
no email disconnect Discontinues sending email alerts upon closing a connect	no email connect	
	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:13) 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.

connect (tunnel-connect:12) level commands	
write	Stores the current configuration in permanent memory.
	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>
start character <control></control>	Sets the connect mode start character. The character may be input as text, control, decimal, or
show status	Displays tunnel connect status.
show history	Displays the last 20 commands entered during the current CLI session.
show	Displays the current configuration.
reconnect time <milliseconds></milliseconds>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.</milliseconds>
promote host < number >	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
local port < <i>number</i> >	Sets a specific port for use as the local port. <number> = the number of the port to use.</number>
kill connection	Disconnects the active connect mode tunneling connection or connections.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
host mode sequential	Connects to the first host in the list that accepts the connection.
host <instance></instance>	Enters the next lower level. Specify the instance for the next lower level.
flush start character enable	Disables forwarding of the connect start character into the network.
flush start character disable	Enables forwarding of the connect start character into the network.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
exit	Returns to the tunnel level.
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>
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>
default start character	Defaults the connect mode start character.

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. <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 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>	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 < 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></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: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).
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:8) level commands	
connect (tunnel-connect:8) level commands block network disable	Forwards (tunnels) network data in connect mode tunneling.
	· · · · · · · · · · · · · · · · · · ·
block network disable	ing.  Discards all data coming in from the connect mode tunnel before forwarding
block network disable block network enable	ing.  Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block network disable block network enable block serial disable	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debug-
block network disable block network enable block serial disable block serial enable	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
block network disable block network enable block serial disable block serial enable clrscrn	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling
block network disable block network enable block serial disable block serial enable clrscrn connect mode always	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial
block network disable  block serial disable  block serial enable  clrscrn  connect mode always  connect mode any character	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
block network disable block network enable block serial disable block serial enable  clrscrn connect mode always  connect mode any character  connect mode disable	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).  Disables connect mode tunneling.  Enables the tunneling server to make tunneling connections when the modem
block network disable block serial disable block serial enable  clrscrn connect mode always  connect mode any character  connect mode disable connect mode modem control asserted	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).  Disables connect mode tunneling.  Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
block network disable block serial disable block serial enable  clrscrn connect mode always connect mode any character  connect mode disable connect mode modem control asserted	ing.  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 tunneling.  Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).  Clears the screen.  Enables the tunneling server to always establish tunneling connections.  Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).  Disables connect mode tunneling.  Enables the tunneling server to make tunneling connections when the modem control pin is asserted.  Enables modem emulation for connect mode tunneling.  Enables connect mode tunneling when the configured start character

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></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 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>	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 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 < 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.
	connect mode turnier.

	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.

host mode sequential	Connects to the first host in the list that accepts the con-
host mode simultaneous	nection.
	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>
	Stores the current configuration in permanent memory.

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 < 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>	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	
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: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. <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:1) 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.
credentials (ssl-credentials) level commands	
credentials (ssl-credentials) level commands clrscrn	Clears the screen.
	Clears the screen.  Create a new credential name
clrscrn	
clrscrn create <credential name=""></credential>	Create a new credential name
clrscrn create <credential name=""> delete <credential name=""></credential></credential>	Create a new credential name  Delete existing credential by name
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <show< td=""><td>Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current</td></show<></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit show show history</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit show show history write</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <show (device)="" commands<="" device="" history="" level="" show="" td="" write=""><td>Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.</td></show></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit show show history write device (device) level commands auto show tlog</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <show (device)="" auto="" clrscrn<="" commands="" device="" history="" level="" show="" td="" tlog="" write=""><td>Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.</td></show></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit show show history write device (device) level commands auto show tlog clrscrn exit</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <show (device)="" auto="" clrscrn="" commands="" device="" exit="" history="" level="" show="" show<="" td="" tlog="" write=""><td>Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information</td></show></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <show (device)="" auto="" clrscrn="" commands="" device="" exit="" hardware="" history="" information<="" level="" show="" td="" tlog="" write=""><td>Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current</td></show></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <show (device)="" auto="" clrscrn="" commands="" device="" exit="" hardware="" history="" history<="" information="" level="" show="" td="" tlog="" write=""><td>Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current CLI session.</td></show></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current CLI session.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit <credential name=""> exit show show history write device (device) level commands auto show tlog clrscrn exit show show hardware information show history show lines</credential></credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current CLI session.  Show line information
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit show show history write device (device) level commands auto show tlog clrscrn exit show show hardware information show history show lines show memory</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current CLI session.  Show line information  Displays current memory usage information.
clrscrn create <credential name=""> delete <credential name=""> edit <credential name=""> exit show show history  write  device (device) level commands auto show tlog clrscrn exit show show hardware information show history  show lines show memory show task state</credential></credential></credential>	Create a new credential name  Delete existing credential by name  View or edit an existing profile  Exits to the ssl level.  Show existing credential names  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Continuously displays the internal trouble log.  Clears the screen.  Exit to the enable level.  Show system information  Displays information about the hardware.  Displays the last 20 commands entered during the current CLI session.  Show line information  Displays current memory usage information.  Displays current task states.

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 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: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 for-
Thus it stop character chaste	warded to the network.
modem control disable	warded to the network.  Does not watch the modem control pin to disconnect.

	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	
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:13) 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.
write disconnect (tunnel-disconnect:12) level commands	Stores the current configuration in permanent memory.
	Stores the current configuration in permanent memory.  Clears the screen.
disconnect (tunnel-disconnect:12) level commands	
disconnect (tunnel-disconnect:12) level commands clrscrn	Clears the screen.
disconnect (tunnel-disconnect:12) level commands clrscrn exit	Clears the screen.  Returns to the tunnel level.  Does not flush serial data upon closing a tunneling con-
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable	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
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush serial enable	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.
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush serial enable flush stop character disable	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 for-
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush serial enable flush stop character disable flush stop character enable	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.
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush serial enable flush stop character disable flush stop character enable modem control disable	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
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush serial enable flush stop character disable flush stop character enable modem control disable modem control enable	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.
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush serial enable flush stop character disable flush stop character enable modem control disable modem control enable no stop character	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
disconnect (tunnel-disconnect:12) level commands clrscrn exit flush serial disable flush stop character disable flush stop character enable modem control disable modem control enable no stop character no timeout	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.

	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.  Stores the current configuration in permanent memory.</milliseconds>
	specified length of time. <milliseconds> = timeout in milliseconds.</milliseconds>
	<milliseconds> = timeout in milliseconds.</milliseconds>
write	Stores the current configuration in permanent memory
	otores the current configuration in permanent memory.
disconnect (tunnel-disconnect:11) level commands	
clrscrn	Clears the screen.
exit	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.
flush stop character disable	Forwards the stop character from the Line to the network.
	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.
I I	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
	Displays the last 20 commands entered during the current CLI session.
	Sets the stop character.
1	The character may be input as text, control, decimal, or hex.
	A control character has the form <control>C.</control>
	A decimal value character has the form \99.
	A hex value character has the form 0xFF.
	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 commands	
clrscrn	Clears the screen.
exit	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.
flush stop character disable	Forwards the stop character from the Line to the network.
	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.
1	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
1	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 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:8) 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.

	T
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: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	
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:5) 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.</control>
	A hex value character has the form 0xFF.
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) 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: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></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.
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.
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 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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from toxt	Sets the From address for email alerts.
from <text></text>	Sets the Fight address for email alerts.

	<text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 12 (email:12) 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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
message file <text></text>	Specifies a text file, the contents of which will be the mes-

no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.

email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port < number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port < <i>number</i> >	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 16 (email:16) 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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <pre><number> = port used for SMTP on the server side.</number></pre>
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 2 (email:2) 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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
message file <text></text>	Specifies a text file, the contents of which will be the message body

Restores the email counters to the aggregate values.  Removes the From address for email alerts.  Removes the file name, so the message body will be empty.  Removes the file name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Attention of the device of t		of an email alert. <text> = the name of a local file.</text>
Removes the From address for email alerts.  Removes the file name, so the message body will be empty.  Removes the file name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Repby To address for email alerts.  Removes subject used for email alerts.  Removes subject used for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Text> = domain name to override the current domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Sets X-Priority for email alerts to 3 (normal).  Priority low  Sets X-Priority for email alerts to 4 (low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets X-Priority for email alerts to 6 (very low).  Sets the Reply To address for email alerts.  Sets the port used by the SMTP server.  Sets the port used for SMTP on the server side.  Displays the current configuration.  Sets the port used for SMTP on the server side.  Displays the email log.  Sets the subject or email alerts.  Sets to addresses for email alerts.  Sets to addresses for email alerts.  S	no cc	Removes the Cc addresses for email alerts.
Removes the file name, so the message body will be empty.  no overriding domain  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes the Reply To address for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Sets Admain name to override the current domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Priority low  Sets X-Priority for email alerts to 4 (low).  Sets X-Priority for email alerts to 4 (low).  Sets X-Priority for email alerts to 1 (urgent).  Sets X-Priority for email alerts to 1 (urgent).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  Sets the port used by the SMTP server.  Sets the port used by the SMTP server.  Sets the port used for SMTP on the server side.  Displays the current configuration.  Show Displays the current configuration.  Show I Displays the email log.  Show statistics  Displays the email log.  Sets the Subject for email alerts.  Sets the Subject for email alerts.  Setx = a quoted, semicolon separated list of email addresses and the subject.  Setx = a quoted, semicolon separated list of email addresses.  C <fext> Sets the current configuration in permanent memory.  Setx = a quoted, semicolon separated list of email addresses.  C clear and counters  C clears the screen.  Sets the email counters to zero.  Clears the screen.</fext>	no clear mail counters	Restores the email counters to the aggregate values.
empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  In the control of the device's domain name in EHLO.  In the control of the current domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Sets X-Priority for email alerts to 4 (low).  In priority low  Sets X-Priority for email alerts to 4 (low).  Sets X-Priority for email alerts to 4 (low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 6 (low).  Sets X-Priority for email alerts to 6 (low).  Sets X-Priority for email alerts to 6 (low).  Sets X-Priority for email alerts to 7 (urgent).  Sets the Reply To address for email alerts.  Sets to email alert.  Sets the Reply To address to place in the Reply To field of the email alert.  Sends an email using the current settings.  Sets the port used for SMTP on the server side.  Show  Displays the current configuration.  Displays the last 20 commands entered during the current cut session.  Show log  Displays the email log.  Show statistics  Displays email statistics.  Sets to addresses for email alerts.  Letx! = a quoted, semicolon separated list of email addresses.  Sets to addresses for email alerts.  Letx! = a quoted, semicolon separated list of email addresses.  Colear mail counters  Clears the screen.  Sets the email counters to zero.  Clears the screen.  Sets the local port (used to send email alerts) to random.	no from	Removes the From address for email alerts.
Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current domain name in EHLO.  Atex1> adomain name to override the current provide the current provide to set the Reply To address for email alerts.  Atex1> adomain name to override the current provide the set of the Reply To addresses for email alerts.  Atex1> adomain name to override the current provide the	no message file	
Removes tubject no to Removes the To addresses for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert insitead of the device's domain name in EHLO.  In the EHLO.  Sets X-Priority for email alerts to 2 (high).  Priority high Sets X-Priority for email alerts to 2 (high).  Priority low Sets X-Priority for email alerts to 4 (low).  Priority orgent Sets X-Priority for email alerts to 1 (urgent).  Priority very low Sets X-Priority for email alerts to 1 (urgent).  Priority very low Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  Set X-ext> = email address to place in the Reply To field of the email alert.  Sends an email using the current settings.  Sets the port used by the SMTP server.  Anumber> = port used for SMTP on the server side.  Show history Displays the current configuration.  Displays the last 20 commands entered during the current CLI session.  Show log Displays the last 20 commands entered during the current CLI session.  Show statistics Displays email statistics.  Sets the Subject for email alerts.  Sets to addresses for email alerts.  Setx = a quoted, semicolon separated list of email addresses.  Set ST o addresses for email alerts.  Setx = a quoted, semicolon separated list of email addresses.  Set ST o addresses for email alerts.  Setx = a quoted, semicolon separated list of email addresses.  Setx = a quoted, semicolon separated list of email addresses.  Setx = a quoted, semicolon separated list of email addresses.  Setx = a quoted, semicolon separated	no overriding domain	Removes the overriding domain name option.
Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Sets X-Priority for email alerts to 3 (normal).  Priority urgent  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 4 (low).  Sets X-Priority for email alerts to 1 (urgent).  Priority urgent  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  **ctext>** email address to place in the Reply To field of the email alert.  **send** Sends an email using the current settings.  Sends an email using the current settings.  Sets the port used by the SMTP server.  **snumber>** Sets the port used by the SMTP on the server side.  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.  **ctext>** etext to placed as the subject.  Sets To addresses for email alerts.  **ctext>** etext to placed as the subject.  Sets To addresses for email alerts.  **ctext>** etext to placed as the subject.  Sets To addresses for email alerts.  **stext>** etext to placed as the subject.  Sets To addresses for email alerts.  **stext>** etext to placed as the subject.  Sets To addresses for email alerts.  **stext>** etext to placed as the subject.  Sets To addresses for email alerts.  **stext>** etext to placed as the subject.  Sets To addresses for email alerts.  **stext>** etext to placed, semicolon separated list of email addresses.  Stores the current configuration in permanent memory.  **stext>** etext to placed, semicolon separated list of email addresses.  Sets Ca addresses for email alerts.  **stext>** extext to addresses for email alerts.  **stext>**	no reply to	Removes the Reply To address for email alerts.
Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  In the server to send an email alert instead of the device's domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Sets X-Priority for email alerts to 2 (high).  Sets X-Priority for email alerts to 3 (normal).  Sets X-Priority for email alerts to 3 (normal).  Sets X-Priority for email alerts to 3 (normal).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  In the send Sends an email using the current settings.  Sets the Reply To address to place in the Reply To field of the email alert.  Sets the port used for SMTP on the server side.  Show Show history  Sets the port used for SMTP on the server side.  Displays the current configuration.  Displays the last 20 commands entered during the current CLI session.  Displays the email log.  Displays the email log.  Displays the email alerts.  In the server server be a quoted, semicolon separated list of email addresses.  Sets the Subject for email alerts.  In the server ser	no subject	Removes subject used for email alerts.
an SMTP server to send an email alert instead of the device's domain name in EHLO. <a href="https://doi.org/10.1001/journ.com/">device's domain name in EHLO.</a> <a href="https://doi.org/">device/<a href="https://doi.org/">device/<a href="https://doi.org/">device/<a href="https://doi.org/">device/<a href="https://doi.org/">device/<a href="https://doi.org/">device/<a "="" doi.org="" href="https://doi.org/&lt;a href=" https:="">device/<a href="https://doi.org/">device/<a href="https://doi.org/">device/</a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>		

to <text></text>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email ad-</text>
subject <text></text>	Sets the Subject for email alerts. <text> = text to placed as the subject.</text>
show statistics	Displays email statistics.
show log	Displays the email log.
show history	Displays the last 20 commands entered during the current CLI session.
show	Displays the current configuration.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
send	Sends an email using the current settings.
	<text> = email address to place in the Reply To field of the email alert.</text>
priority very low reply to <text></text>	Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.
priority very low	Sets X-Priority for email alerts to 1 (urgent).
priority urgent	Sets X-Priority for email alerts to 3 (normal).
priority low	Sets X-Priority for email alerts to 4 (low).
priority high	Sets X-Priority for email alerts to 2 (high).
	name in EHLO.
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 device's domain name in EHLO. <text> = domain name to override the current domain</text>
no to	Removes the To addresses for email alerts.
no subject	Removes subject used for email alerts.
no reply to	Removes the Reply To address for email alerts.
no overriding domain	Removes the overriding domain name option.
no message file	Removes the file name, so the message body will be empty.
no from	Removes the From address for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no cc	Removes the Cc addresses for email alerts.
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>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
exit	Exits to the enable level.
email < <i>number</i> >	Enters the configure email level.
	side.

Sets Cc addresses for email alerts.    Sets Cc addresses for email alerts.   Sets Cc addresses for email alerts.   Sets Cc addresses for email alerts.   Sets the Set al quoted, semicolon separated list of email addresses.   Clears all entries from the mail log.   Clears all entries from the mail log.   Clears the screen.   Sets the email counters to zero.   Clears the screen.   Sets the local port (used to send email alerts) to random.   Sets X-Priority for email alerts to 3 (normal).   Sets addresses for email alerts.   Sets the factory default port for SMTP on the server side.   Enters the configure email evel.   Sets the form address for email alerts.   Sets the form address for email alerts.   Sets the form address for email alerts.   Sets the form address to place in the From field of the email alert.   Sets the form address for email alerts.   Sets the focal port used to send email alerts.   Sets the focal port used to send email alerts.   Sets the focal port used to send email alerts.   Sets the focal port to use for email alerts.   Sets the focal port to use for email alerts.   Sets the focal port to use for email alerts.   Sets the focal port to use for email alerts.   Sets the focal port to use for email alerts.   Sets the name of a local file.   Removes the Cc addresses for email alerts.   Sets and the file name, so the message body will be empty.   Sets and the file name, so the message body will be empty.   Sets and the file name, so the message body will be empty.   Sets and the file name of the set of email alerts.   Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.   Sets X-Priority for email alerts to 2 (high).   Sets X-Priority for email alerts to 3 (normal).   Sets X-Priority for email alerts to 4 (low).   Sets X-Priority for email alerts to 5 (well).   Sets X-Priority for email alerts to 6 (low).   Sets X-Priority for email alerts to 1 (urgent).   Sets X-Priority for email alerts to 3 (normal).   Sets X-	email 5 (email:5) level commands	
clear log   Clears all entries from the mail log.   Clears all entries from the mail log.   Clear all entries from the mail log.   Clears the screen.   Clears the factory default port for SMTP on the server side.   Clears the factory default port for SMTP on the server side.   Clears the configure email alerts to 3 (normal).   Clears the configure email elevel.   Clears the configure email elevel.   Clears the from address for email alerts.   Clears the from a clear fro	auto show statistics	Continuously displays email statistics.
clear mail counters  Clears the screen.  Clears the screen.  Clears the screen.  Clears the screen.  Sets the local port (used to send email alerts) to random. default priority  Sets X-Priority for email alerts to 3 (normal).  Restores the factory default port for SMTP on the server side.  Enters the configure email level.  Exits to the enable level.  Sets the From address for email alerts. <text> = text&gt; = text = te</text>	cc <text></text>	<text> = a quoted, semicolon separated list of email ad-</text>
Clears the screen.  Clears the screen.  Clears the screen.  Sets the local port (used to send email alerts) to random.  Sets X-Priority for email alerts to 3 (normal).  Restores the factory default port for SMTP on the server side.  Enters the configure email level.  Exits to the enable level.  Sets the From address for email alerts.  **clext*>  Sets the From address for email alerts.  **clext*> email address to place in the From field of the email alert.  **clext*> email address to place in the From field of the email alert.  **clext*> email address to place in the From field of the email alert.  **clext*> email address to place in the From field of the email alert.  **clext*> email alert to use for email alerts.  **Sets the local port use for email alerts.  **Specifies a text file, the contents of which will be the message body of an email alert.  **clext*> = the name of a local file.  **Text*> the name of a local file.  **Removes the Ca addresses for email alerts.  **Restores the email counters to the aggregate values.  **no from Removes the From address for email alerts.  **Removes the From address for email alerts.  **Removes the From address for email alerts.  **Removes the Rephy To address for email alerts.  **Removes the Rephy To address for email alerts.  **Removes subject used for email alerts.  **Sets a domain name that will be used when connecting to an SMTP server to an email alert instead of the device's domain name in EHLO.  **Address** domain name to override the current domain name in EHLO.  **Address** domain name to override the current domain name in EHLO.  **Sets X-Priority for email alerts to 1 (urgent).  **Sets X-Priority for email alerts to 1 (urgent).  **Sets X-Priority for email alerts to 5 (very low).  **Sets X-Priority for email alerts to 5 (very low).  **Sets X-Priority for em	clear log	Clears all entries from the mail log.
Sets the local port (used to send email alerts) to random.	clear mail counters	Sets the email counters to zero.
default priority  Sets X-Priority for email alerts to 3 (normal).  Restores the factory default port for SMTP on the server side.  Enters the configure email level.  Exits to the enable level.  Sets the From address for email alerts.	clrscrn	Clears the screen.
Restores the factory default port for SMTP on the server side.	default local port	Sets the local port (used to send email alerts) to random.
side. Enters the configure email level. Exits to the enable level.  Exits to the enable level.  Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.  Sets the local port used to send email alerts. <number>   Sets the local port used to send email alerts. <number>   Sets the local port to use for email alerts. <number>   Secifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.  Removes the Cc addresses for email alerts.  Restores the email counters to the aggregate values.  Removes the From address for email alerts.  Removes the file name, so the message body will be empty.  Removes the file name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes the To addresses for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Diriority low  Sets X-Priority for email alerts to 3 (normal).  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 X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  **enable x-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  **enable x-Priority for email alerts.  **enable x-Priorit</text></number></number></number></text>	default priority	Sets X-Priority for email alerts to 3 (normal).
Exits to the enable level.  Sets the From address for email alerts.  -text> = email address to place in the From field of the email alert.  -text> = email address to place in the From field of the email alert.  -text> = text file, the contents of which will be the message file < text> = sage body of an email alert.  -text> = the name of a local file.  -no cc	default server port	
Sets the From address for email alerts.	email <number></number>	Enters the configure email level.
ctexts = email address to place in the From field of the email alert.	exit	Exits to the enable level.
<ul> <li>-number&gt; local port to use for email alerts.     </li> <li>Specifies a text file, the contents of which will be the message body of an email alert.     </li> <li>-text&gt; = the name of a local file.     </li> <li>Removes the Cc addresses for email alerts.     </li> <li>Restores the email counters to the aggregate values.     </li> <li>no clear mail counters     </li> <li>Removes the From address for email alerts.     </li> <li>Removes the file name, so the message body will be empty.     </li> <li>no overriding domain     </li> <li>Removes the overriding domain name option.     </li> <li>Removes the Reply To address for email alerts.     </li> <li>Removes the To addresses for email alerts.     </li> <li>Removes the To addresses for email alerts.     </li> <li>Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.     </li> <li>-text&gt; = domain name to override the current domain name in EHLO.     </li> <li>Sets X-Priority for email alerts to 2 (high).     </li> <li>Description of the mail alerts to 4 (low).     </li> <li>Sets X-Priority for email alerts to 3 (normal).     </li> <li>Sets X-Priority for email alerts to 5 (very low).     </li> <li>Sets X-Priority for email alerts to 5 (very low).     </li> <li>Sets X-Priority for email alerts to 5 (very low).     </li> <li>Sets the Reply To address for email alerts.     </li> <li>-text&gt; = email address to place in the Reply To field of the email alert.     </li> <li>Send     </li> <li>Send an email using the current settings.     </li> <li>Sets the port used by the SMTP server.     </li> <li>-number&gt; = port used for SMTP on the server side. </li> </ul>	from <text></text>	<text> = email address to place in the From field of the</text>
sage body of an email alert. <text> = the name of a local file.  Removes the Cc addresses for email alerts.  no cc Removes the email counters to the aggregate values.  Restores the email counters to the aggregate values.  Removes the From address for email alerts.  Removes the File name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes the Reply To address for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  <text> = domain name to override the current domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Depositive to the server of the serve</text></text>	local port <number></number>	· ·
Restores the email counters to the aggregate values.  Removes the From address for email alerts.  Removes the From address for email alerts.  Removes the file name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  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.  Sets the Port used by the SMTP server.  Sets the Port used by the SMTP on the server side.	message file <text></text>	of an email alert.
Removes the From address for email alerts.  Removes the file name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Atext> = domain name to override the current domain name in EHLO.  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 X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets the Reply To address for email alerts.  Atext> = email address to place in the Reply To field of the email alert.  Sends an email using the current settings.  Sets the port used by the SMTP server.  Anumber> = port used for SMTP on the server side.	no cc	Removes the Cc addresses for email alerts.
Removes the From address for email alerts.  Removes the file name, so the message body will be empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Alext> = domain name to override the current domain name in EHLO.  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 X-Priority for email alerts to 5 (very low).  Sets X-Presonable for email alerts.  Sets the Reply To address for email email alerts.  Sets the Reply To address for email	no clear mail counters	Restores the email counters to the aggregate values.
empty.  Removes the overriding domain name option.  Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO.  Oriority high Sets X-Priority for email alerts to 2 (high).  Priority low 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).  Sets the Reply To address for email alerts.  Sets the Reply To address for email alerts.  Sets X-Priority for email alerts.  Sets the Reply To address for email alerts.  Sets X-Priority for email alerts.  Sets X-Priority for email alerts.  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).	no from	
Removes the Reply To address for email alerts.  Removes subject used for email alerts.  Removes subject used for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.  Sets X-Priority for email alerts to 2 (high).  Sets X-Priority for email alerts to 4 (low).  Sets X-Priority or email alerts to 3 (normal).  Sets X-Priority or email alerts to 1 (urgent).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  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.  Send  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text></text>	no message file	
Removes subject used for email alerts.  Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.  oriority high  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 X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  Sets K-Priority for email alerts to 5 (very low).  Sets M-Reply To address for email alerts.  <text> = email address to place in the Reply To field of the email alert.  Send  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text></text>	no overriding domain	Removes the overriding domain name option.
Removes the To addresses for email alerts.  Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.  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 urgent  Sets X-Priority for email alerts to 1 (urgent).  Sets X-Priority for email alerts to 5 (very low).  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.  Send  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text></text>	no reply to	Removes the Reply To address for email alerts.
Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.  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 X-Priority for email alerts to 5 (very low).  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.  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text></text>	no subject	Removes subject used for email alerts.
an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.  priority high  priority low  priority low  priority normal  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 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.  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text></text>	no to	Removes the To addresses for email alerts.
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 3 (normal).  Sets X-Priority for email alerts to 1 (urgent).  Sets X-Priority for email alerts to 5 (very low).  Sets X-Priority for email alerts to 5 (very low).  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.  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text>	overriding domain <text></text>	send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain</text>
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 1 (urgent).  Sets X-Priority for email alerts to 5 (very low).  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.  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text>	priority high	Sets X-Priority for email alerts to 2 (high).
priority urgent  Sets X-Priority for email alerts to 1 (urgent).  Sets X-Priority for email alerts to 5 (very low).  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.  Send  Sends an email using the current settings.  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></text>	priority low	Sets X-Priority for email alerts to 4 (low).
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.  Sends an email using the current settings.  Server port <number>  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></number></text>	priority normal	Sets X-Priority for email alerts to 3 (normal).
Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.  Send  Sends an email using the current settings.  Server port <number>  Sets the port used by the SMTP server.  <number> = port used for SMTP on the server side.</number></number></text>	priority urgent	Sets X-Priority for email alerts to 1 (urgent).
<text> = email address to place in the Reply To field of the email alert. send Sends an email using the current settings. Server port <number> Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number></number></text>	priority very low	Sets X-Priority for email alerts to 5 (very low).
Server port <number> Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number></number>	reply to <text></text>	<text> = email address to place in the Reply To field of the</text>
<number> = port used for SMTP on the server side.</number>	send	Sends an email using the current settings.
show Displays the current configuration.	server port <number></number>	
	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.
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port < <i>number</i> >	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port <number></number>	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.

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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port < <i>number</i> >	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>

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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port <number></number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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 local port	Sets the local port (used to send email alerts) to random.

default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <number></number>	Enters the configure email level.
exit	Exits to the enable level.
from <text></text>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.</text>
local port < <i>number</i> >	Sets the local port used to send email alerts. <number> local port to use for email alerts.</number>
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 from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
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.
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 device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.</text>
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.
server port < number>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.</number>
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>

auto show interfaces auto show processes Continuously show thread runtime information closcrin Clears the screen.  configure Enters the configuration level.  connect Show name and number for lines.  connect line <li>connect line </li> <li>device Enters the device level.  disable Exits the enable level.  disable Exits the enable level.  exit the enable level.  Enters the flesystem Enters the filesystem level.  Kills SSH session with index from "show sessions"  Kills telnet <ession> Kills Telnet session with index from "show sessions"  Kills Telnet session with index from "show sessions"  Kills Telnet session with index from "show sessions"  Fenters the line level.  <inne> Inters the line level.  <inne> = number of the line (serial port) to be configured.  Ping destination on times with 5 second timeout  Ping destination in times with 5 second timeout  Ping destination in times with x timeout (in seconds)  reload Reboot system  reload factory defaults to permanent storage  show Show interface statistics  show interfaces Show interface statistics  show interfaces Show interface statistics  show upp/TCP state information  show processes Show thread runtime information  show processes Show thread runtime information Show processes Show thread runtime information Show processes Show Enters the SSH configuration level.  Begin SSH session on network &lt; host&gt;  Begin SSH session on network &lt; hosts.  Begin SSH session on network &lt; hosts.</inne></inne></ession></li>
auto show processes  Clears the screen.  Clears the screen.  Clears the screen.  Configure  Enters the configuration level.  Show name and number for lines.  Connect Iline < line>  Begin session on serial port.  device Enters the device level.  disable Exits the enable level.  disable Exits the enable level.  disable Exits the configure email level.  exit Enters the Configure email level.  Exit from the system  Enters the filesystem level.  Kills SSH session with index from "show sessions"  Kills SSH session with index from "show sessions"  Kills Telnet session with index from "show sessions"  Inter the line level. <inine> = number of the line (serial port) to be configured.  Ping destination continuously with 5 second timeout  Ping   Ping destination in times with 5 second timeout  Ping destination in times with x timeout (in seconds)  reload factory defaults  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 curren CLI session.  Show interfaces  Show interface statistics  Show UDP/TCP state information  Show processes  Show University entered the session show active Telnet and SSH Sessions  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Begin SSH session on network <host></host></inine>
clrscrn  Clears the screen.  configure  Enters the configuration level.  connect  Show name and number for lines.  Begin session on serial port.  device  Enters the device level.  disable  Exits the enable level.  dns  Enters the DNS level.  Enters the configure email level.  exit  Exit from the system  Enters the filesystem level.  kill ssh <session>  Kills SSH session with index from "show sessions"  Kills Telnet session with index from "show sessions"  Kills Telnet session with index from "show sessions"  Kills Telnet session with index from "show sessions"  Fine  <li>Ine </li> <li>Ine </li></session>
configure Enters the configuration level.  connect Show name and number for lines.  connect line <li>Begin session on serial port.  device Enters the device level.  disable Exits the enable level.  dns Enters the DNS level.  email <number> Enters the configure email level.  exit Exit from the system  filesystem Enters the filesystem level.  kill ssh <session> Kills SSH session with index from "show sessions"  kill telnet <session> Kills Telnet session with index from "show sessions"  kill telnet <session> Enters the file level.  <li>cline&gt; = number of the line (serial port) to be configured.  ping <host> count&gt; Ping destination ontinuously with 5 second timeout  ping <host> count&gt; Ping destination in times with 5 second timeout  ping <host> count&gt; Ping destination in 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 curren CLI session.  show interfaces Show UDP/TCP state information  show processes  show lines Show lines Information  show processes  show we reload SSH Sessions  Enters the SSH configuration level.  ssh <ol> <li>sping sSH session on network <host></host></li> <li>Begin SSH session on network <host></host></li> </ol> </host></host></host></li></session></session></session></number></li>
connect line <li>Show name and number for lines.</li> <li>connect line <li>Begin session on serial port.</li> <li>device</li> <li>Enters the device level.</li> <li>disable</li> <li>Exits the enable level.</li> <li>dns</li> <li>Enters the DNS level.</li> <li>email <number></number></li> <li>exit</li> <li>Enters the configure email level.</li> <li>exit</li> <li>Exit from the system</li> <li>Enters the filesystem level.</li> <li>kill ssh <session></session></li> <li>kill ssh <session></session></li> <li>kill sthelet <session></session></li> <li>with index from "show sessions"</li> <li>kill telnet <session></session></li> <li>line <li>line&gt;</li> <li>enters the line level.</li> <li><li>line&gt; = number of the line (serial port) to be configured.</li> <li>ping <host></host></li> <li>ping destination continuously with 5 second timeout</li> <li>ping <host></host></li> <li>count&gt; timeout</li> <li>ping destination in times with x timeout (in seconds)</li> <li>reload</li> <li>Reboot system</li> <li>reload factory defaults</li> <li>Reload factory defaults to permanent storage</li> <li>show</li> <li>Show system information</li> <li>show show interfaces</li> <li>show show interface statistics</li> <li>show interfaces statistics</li> <li>show interfaces show uDP/TCP state information</li> <li>show lines</li> <li>show line information</li> <li>show lines</li> <li>show line information</li> <li>show sessions</li> <li>show heread runtime information</li> <li>show sessions</li> <li>show active Telnet and SSH Sessions</li> <li>enters the SSH configuration level.</li> <li>session on network <host></host></li> </li></li></li>
connect line <li>Show name and number for lines.</li> <li>connect line <li>Begin session on serial port.</li> <li>device</li> <li>Enters the device level.</li> <li>disable</li> <li>Exits the enable level.</li> <li>dns</li> <li>Enters the DNS level.</li> <li>email <number></number></li> <li>exit</li> <li>Enters the configure email level.</li> <li>exit</li> <li>Exit from the system</li> <li>Enters the filesystem level.</li> <li>kill ssh <session></session></li> <li>kill ssh <session></session></li> <li>kill sthelet <session></session></li> <li>with index from "show sessions"</li> <li>kill telnet <session></session></li> <li>line <li>line&gt;</li> <li>enters the line level.</li> <li><li>line&gt; = number of the line (serial port) to be configured.</li> <li>ping <host></host></li> <li>ping destination continuously with 5 second timeout</li> <li>ping <host></host></li> <li>count&gt; timeout</li> <li>ping destination in times with x timeout (in seconds)</li> <li>reload</li> <li>Reboot system</li> <li>reload factory defaults</li> <li>Reload factory defaults to permanent storage</li> <li>show</li> <li>Show system information</li> <li>show show interfaces</li> <li>show show interface statistics</li> <li>show interfaces statistics</li> <li>show interfaces show uDP/TCP state information</li> <li>show lines</li> <li>show line information</li> <li>show lines</li> <li>show line information</li> <li>show sessions</li> <li>show heread runtime information</li> <li>show sessions</li> <li>show active Telnet and SSH Sessions</li> <li>enters the SSH configuration level.</li> <li>session on network <host></host></li> </li></li></li>
device Enters the device level.  disable Exits the enable level.  dns Enters the DNS level.  email <number> Enters the configure email level.  exit Exit from the system  Enters the filesystem level.  kill ssh <session> Kills SSH session with index from "show sessions"  kill telnet <session> Kills SSH session with index from "show sessions"  kill telnet <session> Level the line level.  dine&gt; Ping destination continuously with 5 second timeout  ping <host> Ping destination n times with 5 second timeout  ping <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 curren CLI session.  show interfaces Show UDP/TCP state information  show processes Show Universal information  show processes Show thread runtime information  show processes Show active Telnet and SSH Sessions  show sessions Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Begin SSH session on network <host></host></host></host></session></session></session></number>
device Enters the device level.  disable Exits the enable level.  dns Enters the DNS level.  email <number> Enters the configure email level.  exit Exit from the system  Enters the filesystem level.  kill ssh <session> Kills SSH session with index from "show sessions"  kill telnet <session> Kills SSH session with index from "show sessions"  kill telnet <session> Level the line level.  dine&gt; Ping destination continuously with 5 second timeout  ping <host> Ping destination n times with 5 second timeout  ping <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 curren CLI session.  show interfaces Show UDP/TCP state information  show processes Show Universal information  show processes Show thread runtime information  show processes Show active Telnet and SSH Sessions  show sessions Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Begin SSH session on network <host></host></host></host></session></session></session></number>
Enters the DNS level.
email <number> email <number> exit  Exit from the system  Enters the filesystem level.  kill ssh <session>  kill ssh <session>  kills SSH session with index from "show sessions"  kill telnet <session>  kills Telnet session with index from "show sessions"  line <li>line <li>line&gt;  Enters the line level.  <li>line&gt; = number of the line (serial port) to be configured.  Ping destination continuously with 5 second timeout  ping <host> &lt; count&gt;  Ping destination n times with 5 second timeout  ping <host> <count> &lt; 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 curren CLI session.  show interfaces  Show interface statistics  show ip sockets  Show UDP/TCP state information  show brocesses  Show thread runtime information  show sessions  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Begin SSH session on network <host>.</host></count></host></host></li></li></li></session></session></session></number></number>
exit Exit from the system  Enters the filesystem level.  kill ssh <session>  kills SSH session with index from "show sessions"  kill telnet <session>  kills Telnet session with index from "show sessions"  kills Telnet session with index from "show sessions"  line <li>line <li>line &gt;  Enters the line level.  <li>line&gt; = number of the line (serial port) to be configured.  Ping destination continuously with 5 second timeout  Ping destination n times with 5 second timeout  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  biow history  Displays the last 20 commands entered during the curren 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  Enters the SSH configuration level.  ssh <ol> <li>segin SSH session on network <host></host></li> </ol></li></li></li></session></session>
exit Exit from the system  Enters the filesystem level.  kill ssh <session>  kills SSH session with index from "show sessions"  kill telnet <session>  kills Telnet session with index from "show sessions"  kills Telnet session with index from "show sessions"  line <li>line <li>line &gt;  Enters the line level.  <li>line&gt; = number of the line (serial port) to be configured.  Ping destination continuously with 5 second timeout  Ping destination n times with 5 second timeout  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  biow history  Displays the last 20 commands entered during the curren 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  Enters the SSH configuration level.  ssh <ol> <li>segin SSH session on network <host></host></li> </ol></li></li></li></session></session>
filesystem kill ssh <session> kills SSH session with index from "show sessions" kill telnet <session> kills Telnet session with index from "show sessions" kills SSH session on network <host></host></session></session>
kill ssh <session> kill ssh <session> kill telnet <session> kill telnet <session> kills Telnet session with index from "show sessions" kill telnet <session> kills Telnet session with index from "show sessions" line <li>line <li>line&gt; Enters the line level. <li>line&gt; = number of the line (serial port) to be configured. Ping destination continuously with 5 second timeout Ping <host> <count> Ping destination n times with 5 second timeout Ping destination n times with x timeout (in seconds) Reboot system reload Reboot system Reload factory defaults to permanent storage show Show system information Show history Displays the last 20 commands entered during the curren 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 Enters the SSH configuration level. Ssh <optclientusername> <host> Begin SSH session on network <host>.</host></host></optclientusername></count></host></li></li></li></session></session></session></session></session>
Enters the line level.
cline> = number of the line (serial port) to be configured.   ping <host>   Ping destination continuously with 5 second timeout    </host>
ping <host> <count> Ping destination n times with 5 second timeout Ping <host> <count> <ti>Ping destination n times with x timeout (in seconds) Ping destination n times with x timeout (in seconds) Ping destination n times with x timeout (in seconds) Reboot system Reload factory defaults to permanent storage Show Show system information Pisplays 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 active Telnet and SSH Sessions Show active Telnet and SSH Sessions Show coptClientUsername&gt; <host> Reboot system Reboot syst</host></ti></count></host></count></host>
ping <host> <count> <ti>Ping destination n times with x timeout (in seconds)  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 UDP/TCP state information  Show lines Show line information  Show processes Show thread runtime information  Show sessions Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername></ti></count></host>
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 Show coptClientUsername> < host> Begin SSH session on network < host>.
reload factory defaults  Reload factory defaults to permanent storage  Show  Show system information  Displays the last 20 commands entered during the current CLI session.  Show interfaces  Show interface statistics  Show UDP/TCP state information  Show lines  Show line information  Show processes  Show thread runtime information  Show sessions  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
Show system information  Show history  Displays the last 20 commands entered during the current CLI session.  Show interfaces  Show interface statistics  Show UDP/TCP state information  Show lines  Show line information  Show processes  Show thread runtime information  Show sessions  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
show history  Displays the last 20 commands entered during the current CLI session.  Show interfaces  Show interface statistics  Show UDP/TCP state information  Show lines  Show line information  Show processes  Show thread runtime information  Show sessions  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  Ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
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  Enters the SSH configuration level.  ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
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  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  SSH <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
show lines  show line information  show processes  Show thread runtime information  show sessions  Show active Telnet and SSH Sessions  Enters the SSH configuration level.  ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
show processes  Show thread runtime information  show sessions  Show active Telnet and SSH Sessions  ssh  Enters the SSH configuration level.  ssh <optclientusername> <host>  Begin SSH session on network <host>.</host></host></optclientusername>
show sessions Show active Telnet and SSH Sessions  ssh Enters the SSH configuration level.  ssh <optclientusername> <host> Begin SSH session on network <host>.</host></host></optclientusername>
ssh Enters the SSH configuration level. ssh <optclientusername> <host> Begin SSH session on network <host>.</host></host></optclientusername>
ssh <optclientusername> <host> Begin SSH session on network <host>.</host></host></optclientusername>
The optClientUserName must match an SSH Client: Users configuration entry.  Use "" in optClientUserName to prompt for host username and password.
ssh <optclientusername> <host> <port>  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></port></host></optclientusername>
ssl Enters the SSL configuration level.
telnet <host> Begin telnet session on network <host>.</host></host>
telnet <host> <port> Begin telnet session on network <host>:<port>.</port></host></port></host>
trace route <host> Trace route to destination</host>
trace route <host> <protocol></protocol></host>

tunnel <li>line&gt;</li>	Enters the tunnel level. <pre><li><ine> = number of the tunnel line (serial port) to be con- figured.</ine></li></pre>
write	Stores the current configuration in permanent memory.
xml	Enters the XML level.
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
ls <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	Show file system statistics
show history	Displays the last 20 commands entered during the current CLI session.
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.
exit	Returns to the config level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
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.
host 1 (tunnel-connect-host:16:1) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
and deposit key shavedenings	<text> = IP address or host name of the remote host. Ceta the connect typical AES depoint leave with up to 15.</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 punc-

	l. a
	tuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:15:1) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:14:1) level cor	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.

protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	neling connections.  Removes the connect tunnel AES decrypt key.
no address	Removes the remote host address used to establish tun-
exit	Exits to the next higher level.
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
default protocol	Restores the default protocol as "TCP".
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
clrscrn	Clears the screen.
auto show statistics	show connection statistics
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.
	123ABC "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 <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:
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.
	Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:12:1) 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>
Sets the connect tunnel AES decrypt key with up to 16
bytes.
Each byte is represented by two adjacent hex digits.
Bytes may run together or be separated by optional punctuation:
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 punc-
tuation:
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 45 second connect mode TCP keep alive timeout.
Exits to the next higher level.
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 remote port used to establish tunnel connections.
Removes the SSH user name.
Disables the connect mode TCP keep alive timeout.
Removes the VIP name.
Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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

protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:11:1) 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

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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	
F. 5.555. 10P 400	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:9:1) level commands	
nost i (tuillei-connect-nost.9.1) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
	with.
address <text></text>	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</text>
address <text> aes decrypt key <hexadecimal></hexadecimal></text>	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</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:8:1) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:7:1) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:6:1) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
<del></del>	

tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mod tunneling.  Show  Shows the current configuration.  Displays the last 20 commands entered during the current configuration.  Show statistics  show connection statistics  show connections statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.    stext> = SSH user name for use when establishing tunneling connections with other devices.    stext> = SSH user name.   tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.    validate certificate disable   Skips verification of the server certificate when connecting.   validate certificate enable Requires verification of the server certificate when connecting.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the specified Address.   vip enable Makes connections using the specified Address.   vip amme <text> Sets the VIP name.   Sets the VIP name. Sets the virence.   Sets the remote host to establish tunneling connections with.   cast decrypt key <hexadecimal> Sets the connect tunnel AES decrypt key 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 decrypt key <hexadecimal> Sets the connect tunnel AES encrypt key with up to 16 bytes.   Each byte is represented by two adjacent hex digits.</hexadecimal></hexadecimal></text></milliseconds>		
protocol tcp  Uses SSL protocol for connect mode tunneling.  protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses ITelnet protocol (with IAC) for connect mode tunneling.  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 current configuration.  Show statistics  show connection statistics  show connection statistics  show connections statistics  show connections statistics  statistics  show connections trained for use when establishing tunneling connections  with other devices. <a href="https://creativeconds/">https://creativeconds/</a> Enables TCP keep alive for connect mode tunneling and sets the timer.  **emiliseconds>** = timer value, in milliseconds.  Validate certificate disable  Skips verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  Wip enable  Makes connections using the specified Address.  Wip anale <a href="https://creativeconds/">keep using the specified Address.</a> Wip anale <a href="https://creativeconds/">keep using the specified Address.</a> Sets the Tunnel.  Stores the current configuration in permanent memory.  **Nost 1 (tunnel-connect-host-51) level commands**  address <a href="https://creativeconds/">https://creativeconds/</a> Sets the connect tunnel AES decrypt key 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 re	port <number></number>	
protocol tcp protocol tcp aes Uses TCP protocol with AES encryption for connect mode tunneling. protocol tenet Uses TCP protocol with AES encryption for connect mode tunneling. protocol telnet Uses USE Telnet protocol (with IAC) for connect mode tunneling. protocol udp Uses UDP protocol for connect mode tunneling. Show Uses UDP protocol with AES encryption for connect mode tunneling. Show Shows the current configuration. Show shistory Uses UDP protocol with AES encryption for connect mode tunneling. Show shistory Uses UDP protocol with AES encryption for connect mode tunneling. Show shistory Uses UDP protocol with AES encryption for connect mode tunneling. Show shistory Uses UDP protocol with AES encryption for connect mode tunneling. Show shistory Uses USP protocol with AES encryption for connect mode tunneling. Show shistory Uses USP protocol with AES encryption for connect mode tunneling. Show shistory Uses USP protocol with AES encrypt with a show ship and	protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol tcp aes  Uses TCP protocol with AES encryption for connect moditunneling.  Dises Tenet protocol (with IAC) for connect mode tunneling.  Dises UDP protocol for connect mode tunneling.  Dises UDP protocol with AES encryption for connect mode tunneling.  Show  Show Show is current configuration.  Displays the last 20 commands entered during the current configuration.  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.  Letx = SSH user name.  Statistics  Statistics  Sets the SSH user name for use when establishing tunneling connections  with other devices.  Letx = SSH user name.  Statistics  Stati	protocol ssl	Uses SSL protocol for connect mode tunneling.
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mod tunneling.  Show USP with AES encryption for connect mod tunneling.  Show ISP protocol with AES encryption for connect mod tunneling.  Show ISP protocol with AES encryption for connect mod tunneling.  Show ISP protocol with AES encryption for connect mod tunneling.  Show ISP protocol with AES encryption for connect mod tunneling.  Show ISP protocol with AES encryption for connect mod tunneling tunneling connections statistics  Show connection statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.  Letx1 = SSH user name.  Enables TCP keep alive or connect mode tunneling and sets the timer.  Validate certificate disable  Skips verification of the server certificate when connecting.  Vip disable  Vip disable  Makes connections using the specified Address.  Vip enable  Wakes connections using the Specified Address.  Vip enable  Wakes connections using the VIP name.  Stores the current configuration in permanent memory.  Nost 1 (tunnel-connect-host-5:1) level commands  address < text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 1 (tunnel-connect-host-5:1) level commands  address < text>  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Bytes may run together or be separated by optional punc tuation:  123ABC '12 3A BC' 12,3A, BC 12,3a, bc 12;3a, bc 12	protocol tcp	Uses TCP protocol for connect mode tunneling.
ing.  protocol udp  Uses UDP protocol for connect mode tunneling.  protocol udp aes  Uses UDP protocol with AES encryption for connect mod tunneling.  Show  Shows the current configuration.  Show show is 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.  Sets the SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  Vip disable  Wakes connections using the specified Address.  Vip enable  Vip name <text>  Sets the VIP name.  Vip name <text>  Sets the VIP name.  Vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Rost 1 (tunnel-connect-host-5:1) level commands  address <text>  Sets the remote host to establish tunneling connections with.  Letxt = 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.  aes decrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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" 12 3A BC "12 3A BC" 12 3A BC" 12 3A BC "12 3A BC" 12 3</hexadecimal></text></text></text></text></milliseconds></milliseconds>	protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol udp aes  Uses UDP protocol with AES encryption for connect mod tunneling.  Show  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. <te> <te> <te> <te> <te> <te> <te> <te< td=""><td>protocol telnet</td><td>Uses Telnet protocol (with IAC) for connect mode tunneling.</td></te<></te></te></te></te></te></te></te>	protocol telnet	Uses Telnet protocol (with IAC) 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 Show connections statistics Show connections statistics  show connections statistics Show connections with other devices.  stexts — SSH user name for use when establishing tunnelling connections with other devices.  stexts — SSH user name.  top keep alive <milliseconds>  top keep alive for connect mode tunneling and sets the timer.  step keep alive for connect mode tunneling and sets the timer.  step keep alive for connect mode tunneling and sets the timer.  step keep alive for connect mode tunneling and sets the timer.  step keep alive for connect when connecting.  validate certificate disable Skips verification of the server certificate when connecting.  validate certificate enable Requires verification of the server certificate when connecting.  vip disable Makes connections using the specified Address.  what we connection susing the VIP name.  vip name <text>  sets the VIP name.  vip name <text>  sets the VIP name.  vip name <text>  stores the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) 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 "123A BC" 123A, BC 12.3a, bc 12.3a</text></text></text></text></text></milliseconds>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the currer CLI session.  Show statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices. <a 12.3a.bc="" <hexadecimal="" aes="" contains="" decrypt="" enclose="" href="mailto:center-left-state-&lt;/td&gt;&lt;td&gt;protocol udp aes&lt;/td&gt;&lt;td&gt;Uses UDP protocol with AES encryption for connect mode tunneling.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Show statistics  show connection statistics  ssh username &lt;text&gt;  Sets the SSH user name for use when establishing tunneling connections with other devices. &lt;text&gt;= SSH user name.  tcp keep alive &lt;milliseconds&gt;  Enables TCP keep alive for connect mode tunneling and sets the timer. &lt;milliseconds&gt; = 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sores the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) level commands  address &lt;text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt;= 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 punc tuation:  123ABC " if="" it="" key="" must="" note="" quotes="" spaces.="" that="" the="" value="">  Sets the connect tunnel AES decrypt key 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 punc tuation:  Vip the separated by two adjacent hex digits.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc tunnel has part and the punctual and</a>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  validate certificate disable  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) 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.  Bytes may run together or be separated by optional punc tuation:  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 decrypt key 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 two adjacent hex digits.  Bytes may run together or be separated by optional punc tuation:  123 ABC *12 3 ABC *1</text></text></text></milliseconds>	show history	Displays the last 20 commands entered during the current CLI session.
neling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) 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.  aes encrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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 optional punctuations and the server certificate when connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuals.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuals.  Sets the connect tunnel AES en</hexadecimal></text></text></text></milliseconds></milliseconds></text>	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Makes connections using the specified Address.  vip enable  vip name <text> Sets the VIP name.  vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) 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 punc tuation:  123ABC "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 <hexadecimal>  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc</hexadecimal></text></text></text></text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) 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 punc tuation:  123ABC "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 &lt; text&gt;  Sets the connect tunnel AES decrypt key 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 &lt; hexadecimal&gt;  Sets the connect tunnel AES encrypt key 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 punc</text>	validate certificate disable	l. '
vip enable  vip name <text>  Sets the VIP name.  write  Stores the current configuration in permanent memory.  Nost 1 (tunnel-connect-host:5:1) 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 punc tuation:  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 decrypt key 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 punc</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  write  Stores the current configuration in permanent memory.  host 1 (tunnel-connect-host:5:1) 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 punc tuation:  123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc</text></text></text></text>	vip disable	Makes connections using the specified Address.
write  Stores the current configuration in permanent memory.  Nost 1 (tunnel-connect-host:5:1) 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 punc tuation:  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 punc</text>	vip enable	Makes connections using the VIP name.
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 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. Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc</text></text>	vip name <text></text>	Sets the VIP name.
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.  aes decrypt key text &lt; text&gt;  Sets the connect tunnel AES decrypt key 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 punc</text>	write	Stores the current configuration in permanent memory.
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 punc tuation: 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 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 punc</text>	host 1 (tunnel-connect-host:5:1) level commands	
aes decrypt key <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 punc tuation: 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 punc</hexadecimal>	address <text></text>	with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 punc</hexadecimal>	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
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
	aes encrypt key <i><hexadecimal></hexadecimal></i>	bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-

validate certificate disable	Skips verification of the server certificate when connect-
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
ino addiess	Removes the remote host address used to establish tunneling connections.
no address	Exits to the next higher level.
· ·	alive timeout.
default tcp keep alive	Restores the default 45 second connect mode TCP keep
default protocol	client.  Restores the default protocol as "TCP".
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL
clrscrn	Clears the screen.
auto show statistics	show connection statistics
aes encrypt key text < <i>text</i> >	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.
age encrypt key text -text	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

	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:4:1) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.

no ten koon aliko	Disables the connect made TCD keep alive timeseut
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:3:1) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.

	<milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:2:1) 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 <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.
clrscrn credentials <text></text>	Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.
	Selects the RSA/DSA certificates by name for the SSL
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
credentials <text> default protocol</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep
credentials <text>  default protocol  default tcp keep alive</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.
credentials <text>  default protocol  default tcp keep alive  exit</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun-
credentials <text>  default protocol  default tcp keep alive  exit  no address  no aes decrypt key</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.
credentials <text>  default protocol  default tcp keep alive  exit  no address</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.

	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:1:1) level commands address < 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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>

ton koon alivo amillisacandes	Enables TCD keep alive for connect made tuppeling and
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.
	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent 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. <a href="text"><text< a=""> = username.</text<></a>
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:16:10) 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

Sets the connect tunnel AES encrypt key 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		T
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puncturation: 123ABC*123ABC*123ABC*123ABC*123ABC*123AbC*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.  auto show statistics clrscm  Clears the screen.  Clears the screen.  Credentials <fext>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connect to selection.  Removes the remote port used to establish tunnel connect to port used to establish tunnel connect port to use for connect mode tunneling.  Protocol ssh Protocol for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol tep uses the protocol (with IAC) for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tun</fext>		Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics cirscrn Clears the screen. Clears the screen. Clears the screen.  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address Removes the remote host address used to establish tunneling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no credentials Clears the RSA/DSA certificate selection.  no port Removes the connect unnel AES encrypt key.  no credentials Clears the RSA/DSA certificate selection.  no port Removes the sSH user name.  no top keep alive Disables the connect mode TCP keep alive timeout.  no vip name Removes the SSH user name.  Sets the remote port to use for connect mode tunneling.  volumber> Sets the remote port to use for connect mode tunneling.  protocol ssh Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Protocol top Uses TCP protocol for connect mode tunneling.  protocol top uses TCP protocol with AES encryption for connect mode tunneling.  protocol dep protocol dep Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol dep protocol dep Uses UDP protocol for connect mode tunneling.  Protocol dep Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol dep Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
cirsorn  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 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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.  Removes the remote port used to establish tunnel connections.  no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  runmber&gt;  sets the remote port to use for connect mode tunneling.  runmber&gt;  protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP protocol for connect mode tunneling.  protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tep aes  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show bistory  Displays the last 20 commands entered during the current CLI session.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <fext>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt 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 VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SSL protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol telnet  Uses UDP protocol (with IAC) for connect mode tunneling.  Protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp  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.</fext>	auto show statistics	show connection statistics
client.  default protocol  default top keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Ro aes decrypt key  Removes the connect tunnel AES decrypt key.  Ro credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Ro vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssl  Uses SSL protocol for connect mode tunneling.  protocol top  Uses TCP protocol for connect mode tunneling.  protocol top aes  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show the current configuration.  Show the current configuration.  Displays the last 20 commands entered during the current CLI session.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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 SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 TCP 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.  Uses TCP protocol of connect mode tunneling.  Uses USP protocol of connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Protocol udp  Uses USP protocol for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol tep aes  Uses Telnet protocol (with IAC) for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Sets the remote port used to establish tunnel and tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Sets the remote port used to establish tunnel and tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Sets the remote port used to establish tunnel and tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Sets the remote port	credentials <text></text>	
exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  no top keep alive Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp Uses UDP protocol (with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	default protocol	Restores the default protocol as "TCP".
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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> Sets the remote port to use for connect mode tunneling.  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.  Protocol tep aes  Uses Tenet protocol (with IAC) for connect mode tunneling.  Uses Tenet protocol (with IAC) for connect mode tunneling.  Protocol udp  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.	default tcp keep alive	· ·
neling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no aes encrypt key Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <a href="mailto:rnumber">rnumber</a> Sets the remote port to use for connect mode tunneling.  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 UDP protocol for connect mode tunneling.  protocol 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.	exit	Exits to the next higher level.
no aes 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.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh Uses SSH protocol for connect mode tunneling.  Protocol tcp Uses TCP protocol for connect mode tunneling.  Protocol telnet Uses TCP protocol (with IAC) for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp 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.  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  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 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.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Uses TCP 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.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.  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.  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.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  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.  Protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP 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.	no port	
no vip name  Removes the VIP name.  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses TCP protocol for connect mode tunneling.  Uses UDP protocol (with IAC) 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.	no ssh username	Removes the SSH user name.
port <number></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
cnumber> = number of the port to use.   protocol ssh	no vip name	Removes the VIP name.
protocol ssl  protocol tcp  protocol tcp  protocol tcp aes  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.  protocol udp  protocol udp  protocol udp aes  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.	port <number></number>	Sets the remote port to use for connect mode tunneling. <pre></pre> <pre><pre><pre><pre><pre><pre><pr< td=""></pr<></pre></pre></pre></pre></pre></pre>
protocol tcp protocol tcp aes 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.  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.	protocol ssh	Uses SSH 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.  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.	protocol ssl	Uses SSL protocol for connect mode tunneling.
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  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.	protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol udp  protocol udp aes  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.	protocol tcp aes	
protocol udp aes  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.	protocol telnet	i. ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '
tunneling.  show Shows the current configuration.  show history Displays the last 20 commands entered during the current CLI session.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the current CLI session.	protocol udp aes	
CLI session.	show	Shows the current configuration.
show statistics show connection statistics	show history	
	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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:15:10) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:14:10) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:13:10) 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.
	Cloure the solech.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
credentials <text> default protocol</text>	Selects the RSA/DSA certificates by name for the SSL

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:10:10) level co	
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.

	I
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:8:10) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:7:10) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:6:10) 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 < 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 tep ases  Uses TCP protocol with AES encryption for connect mode tunneling.  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Show as UDP protocol with AES encryption for connect mode tunneling.  show  Shows the current configuration.  Shows the current configuration.  Shows 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.  stext = SSH user name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the VIP name.  vip name <text>  write  Rest the VIP name.  Sets the VIP name of the remote host.  Sets the current configuration in permanent memory.  Institute = IP address or host name of the remote host.  Sets the current configuration in permanent memory.  Institute = IP address or host name of the remote host.  Sets the current configuration in permanent memory.  Institute = 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*12.3ABC*12.3abc*12.3abc*12.3abc*  Note that quotes must enclose the value if it contains spaces.  Best the connect tunnel AES encrypt key with up 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*12.3ABC*12.3abc*12.3abc*12.3abc*12.3abc*  Note that quotes must enclose</text></milliseconds>		
ing.    Description   Uses UDP protocol for connect mode tunneling.	protocol tcp aes	
protocol udp aes  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.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  Vip disable  Vip disable  Vip aname <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Stores the current configuration in permanent memory.  Nost 10 (tunnel-connect-host-5:10) level commands  address <text>  Sets the remote host to establish tunneling connections with.  <te> <te> <te> Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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 two adjacent hex 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 encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex 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 mu</te></te></te></text></text></milliseconds></milliseconds>	protocol telnet	l.
show Shows the current configuration.  Show thistory  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.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  - milliseconds&gt; = 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.  vip disable  Makes connections using the specified Address.  vip enable  vip name <text>  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  10st10 (tunnel-connect-inost-5:10) level commands  address <text>  Sets the remote host to establish tunneling connections with.  -text&gt; = 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 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</text></text></milliseconds>	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.	protocol udp aes	
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  <milliseconds> = timer value, in milliseconds.  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the vIP name.  Sets the VIP name.  vip name <text>  Sets the VIP name.  write  Stores the current configuration in permanent memory.  host 10 (tunnel-connect-host-5-10) 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.  aes encrypt key <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 16 bytes.  Each byte is represented by two adjacent hex 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.  aes encrypt key text <text>  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></hexadecimal></text></text></text></milliseconds></milliseconds></text>	show history	
neling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  Validate certificate when connecting.  Validate certificate enable  Requires verification of the server certificate when connecting.  Validate certificate when connections using the view of certificate when connections.  Validate certificate when connections using the view precise.  Validate certificate when connections using the view precise.  Validate certificate when connections.  Validate certificate disable  Makes connections using the view precise.  Validate certificate when connections using the view precise.  Validate certificate when connect undering the view precise.  Sets the remote host to establish tunneling connections with.  **extext**  Sets the remote host to establish tunneling connections with.  **extext**  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC *12,3A,BC 12,3a,bc 12,3a,</milliseconds></milliseconds></text>	show statistics	show connection statistics
sets the timer. <pre><milliseconds> = timer 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Nost 10 (tunnel-connect-host:5:10) level commands**  address < text>  Sets the remote host to establish tunneling connections with. <pre><mitext =="" address="" host="" host.<="" ip="" name="" of="" or="" pre="" remote="" the="">  aes decrypt key </mitext></pre> Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "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   Sets the connect tunnel AES decrypt key 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 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES en	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 10 (tunnel-connect-host:5:10) level commands  address <fext>  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.  aes decrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</hexadecimal></text></fext>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 10 (tunnel-connect-host:5:10) 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.  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "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 two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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.</text></text></text></text></text>	validate certificate disable	l. ·
vip enable vip name <text> Sets the VIP name. Sets the VIP name. Stores the current configuration in permanent memory.  **Note 10 (tunnel-connect-host:5:10) level commands**  address <text>  **Sets the remote host to establish tunneling connections with.  **dext&gt; = 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.  **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.  **Sets the connect tunnel AES encrypt key with up to 16 bytes.  **Each byte is represented by two adjacent hex digits.  **Bytes may run together or be separated by optional punctuation:  **123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc  Note that quotes must enclose the value if it contains spaces.  **323BC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc  Note that quotes must enclose the value if it contains spaces.  **323BC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a.bc  **323BC "12 3A BC</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 10 (tunnel-connect-host:5:10) level commands  address <text>  Sets the remote host to establish tunneling connections with.     Sets the connect tunnel AES decrypt key with up to 16 bytes.    </text></text>	vip disable	Makes connections using the specified Address.
In tunnel-connect-host:5:10) level commands  address < text>  Sets the remote host to establish tunneling connections with.	vip enable	Makes connections using the VIP name.
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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vin name <text></text>	Sats the VIP name
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.  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	INP HAITO STORE	Dets the vir hame.
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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	<u> </u>	
aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></hexadecimal>	write	
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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.</text></hexadecimal>	write host 10 (tunnel-connect-host:5:10) level commands	Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	write 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.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	write host 10 (tunnel-connect-host:5:10) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	write host 10 (tunnel-connect-host:5:10) level commands address <text> aes decrypt key <hexadecimal> aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

Sets the remote host to establish tunneling connections with. <text>= IP address or host name of the remote host.  <text>= le address or host name of the remote host.  <text>= le address or host name of the remote host.  <text>= le address or host name of the remote host.  <text>= le address or host name of the remote host.  <text>= le address or host name of the remote host.  <text>= lead host of the tempte host to establish tunnel and of the remote host.  <text>= lead host of the tempte host to establish tunneling connections.  <text>Beach byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional pun tuation.  123ABC '12 3A BC' 12.3A, BC 12.3a, bc 12.3a, bc 12.3a, bc 12.3a, bc 12.5a, bc 14.5a, 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 pun tuation:  123ABC '12 3A BC' 12.3a, bC 1</text></text></text></text></text></text></text></text></text>	vip name <text></text>	Sets the VIP name.
Sets the remote host to establish tunneling connections with.    Actable   Pladdress or host name of the remote host.	write	Stores the current configuration in permanent memory.
Sets the remote host to establish tunneling connections with.    Actable   Pladdress or host name of the remote host.	host 10 (tunnel-connect-host:4:10) level cor	nmands
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puntuation: 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 puntuation: 123ABC "12.3A.BC 12.3a.bc	address <text></text>	Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional pun tuation: 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 pun tuation: 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 pun tuation: 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.  Clears the screen.  Clears the screen.  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as 'TCP''.  Restores the default 45 second connect mode TCP keep alive timeout.  Exist to the next higher level.  Removes the remote host address used to establish tun neling connections.  Removes the remote bost address used to establish tun neling connections.  Removes the remote bort address used to establish tun neling connections.  Removes the remote port to used to establish tunnel con- nections.  Removes the remote port used to establish tunnel con- nections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect m		
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 punt tuation:  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. 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.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun neling connections.  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 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 used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Cnumber> enumber of the port to use.	aes decrypt key <i><nexadecimai></nexadecimai></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
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 puntuation: 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 encrypt key 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.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun neling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES decrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SH user name.  Disables the connect made TCP keep alive timeout.  Removes the SH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  con and content of the port to use.	aes decrypt key text <text></text>	bytes.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puntuation:  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.  Beauto show statistics  closure close the value if it contains spaces.  Selects the screen.  Clears the screen.  Clears the screen.  Credentials <a href="text">text</a> Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  The connection screen are encrypt 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 SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Sets the remote port to use.		Note that quotes must enclose the value if it contains
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".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun neling connections.  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 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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  <number> = number of the port to use.</number></text>	aes encrypt key <i><hexadecimal></hexadecimal></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Removes the Connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  comber> = number of the port to use.	aes encrypt key text < <i>text</i> >	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  conumber> = number of the port to use.	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  Sets the remote port to use for connect mode tunneling.  <number> = number of the port to use.</number></number>	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  Removes the remote host address used to establish tun neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  enoty	credentials <text></text>	Land to the state of the state
alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  cnumber> = number of the port to use.	default protocol	Restores the default protocol as "TCP".
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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  commber> = number of the port to use.	default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  cnumber> = number of the port to use.	exit	Exits to the next higher level.
Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  connections.	no address	Removes the remote host address used to establish tunneling connections.
Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  conumber> = number of the port to use.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  Sets the remote port to use for connect mode tunneling.  <number> = number of the port to use.</number></number>	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  no vip name  port <number>  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  <number> = number of the port to use.</number></number>	no port	
no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>	no ssh username	Removes the SSH user name.
port < <i>number&gt;</i> Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
<number> = number of the port to use.</number>	no vip name	Removes the VIP name.
protocol ssh Uses SSH protocol for connect mode tunneling.	port <number></number>	
Teach and the first teach	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.
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> tcp keep alive <milliseconds></milliseconds></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and</text>
top receptains strains coorday	sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:3:10) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:2:10) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:1:10) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with. <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre> <pre></pre> <pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre> <pre></pre> <pre> <pre></pre> <pr< td=""></pr<></pre></pre></pre></pre>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-

	ing
validate certificate enable	ing.  Requires verification of the server certificate when con-
validate certificate enable	necting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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. <a href="text"><a 12="" 12,3a,bc="" 12.3a.bc="" 12:3a:bc="" 3a="" bc"="" contains="" enclose="" href="text&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;write&lt;/td&gt;&lt;td&gt;Stores the current configuration in permanent memory.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;host 11 (tunnel-connect-host:16:11) level commands&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;address &lt;text&gt;&lt;/td&gt;&lt;td&gt;Sets the remote host to establish tunneling connections with.  &lt;text&gt; = IP address or host name of the remote host.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;aes decrypt key &lt;hexadecimal&gt;&lt;/td&gt;&lt;td&gt;Sets the connect tunnel AES decrypt key with 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="" must="" note="" quotes="" spaces.<="" td="" that="" the="" value=""></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel con-
	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:14:11) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun-

	neling connections
	with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and
top Roop anve Aminocoonas	sets the timer.
	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:13:11) level command	<u> </u>
address <text></text>	Sets the remote host to establish tunneling connections with.
	<pre><text> = IP address or host name of the remote host.</text></pre>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:12:11) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun-
	neling connections with other devices.
	<pre><text> = SSH user name.</text></pre>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and
	sets the timer.
unlidete negittente diseble	<pre><milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:11:11) 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 punc-
	tuation:
	123ABC "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 punc-
	tuation:   123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.

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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:10:11) 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:

	T
	123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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".

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:8:11) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:7:11) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep
asiaan op noop allve	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:6:11) level co	
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
l	Uses TCP protocol with AES encryption for connect mode
protocol tcp aes	tunneling.

	I
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:4:11) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

host 11 (tunnel-connect-host:2:11) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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 tunne ing. protocol udp  Uses UDP protocol for connect mode tunneling. 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 curre CLI session. Show connection statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices. Letx1> SSH user name.  Enables TCP keep alive for connect mode tunneling an 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.  vip disable  Makes connections using the specified Address. vip enable  Makes connections using the VIP name.  Vip name <text>  Vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Lost 11 (tunnel-connect-host:111) level commands address <text>  Sets the remote host to establish tunneling connections with. </text></text></text>	protocol tcp aes	
protocol udp   Uses UDP protocol for connect mode tunneling.   Uses UDP protocol with AES encryption for connect mode tunneling.   Show	<u> </u>	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol udp aes    Uses UDP protocol with AES encryption for connect motunneling.   Show history	protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
tunneling.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the curn CLI session.  Show statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.   stext> = SSH user name.   tcp keep alive <milliliseconds> Enables TCP keep alive for connect mode tunneling an sets the timer.  <milliliseconds> = timer value, in milliseconds.  validate certificate disable  Skips verification of the server certificate when connect ing.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  vip name <text>  Makes connections using the specified Address.  vip name <text>  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Text=1 (tunnel-connect-host-1:11) level commands*  address <text>  Sets the remote host to establish tunneling connections with.  <text>= IP address or host name of the remote host.  aes decrypt key <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 pur utation:  123ABC "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 <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 pur utation:  123ABC "12 3A BC" 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.  25ets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional pur utation:  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.</hexadecimal></hexadecimal></text></text></text></text></milliliseconds></milliliseconds>	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling an 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.  vip disable  Makes connections using the specified Address.  vip enable  vip name <text>  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Note that (utunnel-connect-host:1:11) level commands*  address &lt; text&gt;  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 pur tuation:  123ABC *123ABC*123ABC*123a.bc*123a.</text></text></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the current CLI session.
neling connections with other devices.   stext> = SSH user name.	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Vip name <text>  Sets the VIP name.  Write  Stores the current configuration in permanent memory.  Nost 11 (tunnel-connect-host:1:11) 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 pur tuation:  123ABC "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 <hexadecimal>  Sets the connect tunnel AES decrypt key 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 pur tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains spaces.</hexadecimal></text></text></text>	tcp keep alive <milliseconds></milliseconds>	
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Itost 11 (tunnel-connect-host:1:11) 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 pur tuation:  123ABC "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 <hexadecimal>  Sets the connect tunnel AES decrypt key 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 pur tuation:  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.</hexadecimal></text></text></text>	validate certificate disable	Skips verification of the server certificate when connecting.
vip enable vip name <text> Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 11 (tunnel-connect-host:1:11) 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 pur tuation:  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 pur tuation:  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 pur tuation:  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></text></text>	validate certificate enable	Requires verification of the server certificate when connecting.
vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 11 (tunnel-connect-host:1:11) 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 pur tuation:  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 pur tuation:  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.</text></text></text>	vip disable	Makes connections using the specified Address.
write   Stores the current configuration in permanent memory.   Iost 11 (tunnel-connect-host:1:11) level commands   Sets the remote host to establish tunneling connections with.     <text></text>	vip enable	Makes connections using the VIP name.
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 pur tuation:  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 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 pur tuation:  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>	vip name <text></text>	Sets the VIP name.
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 pur tuation:  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 pur tuation:  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>	write	Stores the current configuration in permanent memory.
with. <text> = IP address or host name of the remote host.  aes decrypt key <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 pur tuation: 123ABC "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>  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional pur tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.</hexadecimal></text></hexadecimal></text>	host 11 (tunnal-connect-host-1-11) loval commands	
aes decrypt key <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 pur tuation: 123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional pur tuation: 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></hexadecimal>	nost in (turnier-connect-nost. i. ii) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional pur tuation: 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.  aes encrypt key <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 pur tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.</hexadecimal>		1
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 pur tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.</hexadecimal>		with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional pur tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.	address <text></text>	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</text>
Sets the connect tunnel AFS encrypt key with up to 16	address <text> aes decrypt key <hexadecimal></hexadecimal></text>	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</text>
bytes.  Each byte is represented by a single character.	address <text>  aes decrypt key <hexadecimal>  aes decrypt key text <text></text></hexadecimal></text>	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</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (config-host:11) 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. <a href="text"><text> = username.</text></a>
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:16:12) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:15:12) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.

no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:14:12) 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 < <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:13:12) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.

no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:12:12) 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.
I	Sets the connect tunnel AES decrypt key with up to 16
aes decrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

aes encrypt key text < text>  auto show statistics clrscrn	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and

	sets the timer.
validate certificate disable	<pre><milliseconds> = timer value, in milliseconds.</milliseconds></pre> Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:11:12) 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 by optional punctuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:10:12) 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></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 punc-
	tuation:
	123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices.

	<text> = SSH user name.</text>
to a local a Pica and a second	
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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>	Sets the connect tunnel AES decrypt key 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no acc accippt not	restricted the conflict turner /Le decrypt key.

	D 4 14 14 15 14
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:8:12) 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

	1.
	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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

sh username <text></text>	Sets the SSH user name for use when establishing tun-
in domaino storio	neling connections
	with other devices. <text> = SSH user name.</text>
p keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and
p Reep alive Chilliseconds	sets the timer.
	<milliseconds> = timer value, in milliseconds.</milliseconds>
alidate certificate disable	Skips verification of the server certificate when connecting.
alidate certificate enable	Requires verification of the server certificate when connecting.
p disable	Makes connections using the specified Address.
p enable	Makes connections using the VIP name.
p name <text></text>	Sets the VIP name.
rite	Stores the current configuration in permanent memory.
ost 12 (tunnel-connect-host:7:12) level commands	
ddress <text></text>	Sets the remote host to establish tunneling connections with.
	<text> = IP address or host name of the remote host.</text>
es 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.
es 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.
es 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.
es 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
uto show statistics	spaces. show connection statistics
rscrn	Clears the screen.
redentials <text></text>	Selects the RSA/DSA certificates by name for the SSL
odomidis (toxt)	client.
efault protocol	Restores the default protocol as "TCP".
efault tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
xit	Exits to the next higher level.
	Late to the flext fligher level.

	123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc
acc acc.ypt hoy shouldoomlar	bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:
address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
host 12 (tunnel-connect-host:6:12) level commands	Cata the veneta heat to actable to the Cata
write	Stores the current configuration in permanent memory.
vip name <text></text>	Sets the VIP name.
vip enable	Makes connections using the VIP name.
vip disable	Makes connections using the specified Address.
validate certificate enable	Requires verification of the server certificate when connecting.
validate certificate disable	Skips verification of the server certificate when connecting.
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.

	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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".

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:4:12) 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
aes encrypt key <hexadecimal></hexadecimal>	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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:3:12) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:2:12) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 mode
protocol tcp aes	tunneling.

show show shows the current configuration.  Show she current configuration.  Show she statistics  Show connections statistics  Show connections statistics  Show connections with other devices.  Let ye keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  It ye keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  Will is yearification of the server certificate when connecting.  Validate certificate enable  Requires verification of the server certificate when connecting.  Vip disable  Makes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Vip name <fext>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 12 (tunnel-connect-host 112) level commands  address   Sets the remote host to establish tunneling connections with.  Letx'&gt; = 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.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Each byte is represented by two adjacent hex digits.  Each byte is represented by two adjacent hex digits.  Each byte is represented by two adjacent hex digits.</fext></milliseconds></milliseconds>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history    Displays the last 20 commands entered during the currer CLI session.   Show connection statistics	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
cLl session.  show statistics  show connection statistics  ssh username <text>  Sets the SSH user name for use when establishing tunneling connections with other devices.    tcp keep alive <milliseconds>   tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  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  Note that quotes must enclose the value if it contains spaces.  aes decrypt key <a href="#"></a></milliseconds></milliseconds></milliseconds></text>	show	Shows the current configuration.
ssh username <fext>  Sets the SSH user name for use when establishing tunneling connections with other devices. <text>= SSH user name.   tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip enable Makes connections using the VIP name.   vip anme <fext></fext> write Stores the current configuration in permanent memory.   tost 12 (tunnel-connect-host:1:12) level commands   address <fext></fext> sets the remote host to establish tunneling connections with.   aes decrypt key <hexadecimal> Sets the connect tunnel AES decrypt key with up to 16 bytes.   aes decrypt key <fext <fext=""></fext> sets he connect tunnel AES decrypt key with up to 16 bytes.   aes decrypt key text <fext></fext> sets the connect tunnel AES decrypt key with up to 16 bytes.   aes decrypt key text <fext></fext> sets the connect tunnel AES decrypt key with up to 16 bytes.   aes decrypt key text <fext></fext> sets the connect tunnel AES decrypt key with up to 16 bytes.   aes encrypt key <fext 16="" bytes.<="" decript="" key="" td="" to="" up="" vith="">   aes encrypt key text <fext></fext> sets the connect tunnel AES encrypt key with up to 16 bytes.   aes encrypt key text <fext></fext> sets the connect tunnel AES encrypt key with up to 16 bytes.   aes encrypt key text <fext></fext> sets the connect tunnel AES encrypt key with up to 16 bytes.</fext></hexadecimal></milliseconds></milliseconds></text></fext>	show history	Displays the last 20 commands entered during the current CLI session.
neling connections with other devices.	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	neling connections with other devices.
ing.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Sost 12 (tunnel-connect-host:1:12) 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 punct tuation:  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</text></text></text>	tcp keep alive <milliseconds></milliseconds>	
necting.	validate certificate disable	i ·
vip enable       Makes connections using the VIP name.         vip name        Sets the VIP name.         write       Stores the current configuration in permanent memory.         host 12 (tunnel-connect-host:1:12) level commands         address < text>       Sets the remote host to establish tunneling connections with.         .text> = IP address or host name of the remote host.         ses decrypt key < 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>       Sets the connect tunnel AES encrypt key with up to 16 bytes.         Each byte is represented by two adjacent hex 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.         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 th	validate certificate enable	
vip name <text> Sets the VIP name.  write Stores the current configuration in permanent memory.  **Nost 12 (tunnel-connect-host:1:12) level commands**  address <text> Sets the remote host to establish tunneling connections with.  <text> = IP address or host name of the remote host.  aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  123ABC "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 two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.</text></text></hexadecimal></text></text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.	vip enable	Makes connections using the VIP name.
address <text>  Sets the remote host to establish tunneling connections with.    Activate</text>	vip name <text></text>	Sets the VIP name.
aes decrypt key <hexadecimal>  Sets the remote host to establish tunneling connections with.  <text> = IP address or host name of the remote host.   aes decrypt key <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.  Sets the connect tunnel AES decrypt key 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.  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</text></hexadecimal></text></hexadecimal>	write	Stores the current configuration in permanent memory.
with. <text> = IP address or host name of the remote host.  aes decrypt key <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.  Sets the connect tunnel AES decrypt key 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.  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.  Sets the connect tunnel AES encrypt key 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</text></hexadecimal></text>	host 12 (tunnel-connect-host:1:12) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics</text></text>	address <text></text>	with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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</text></hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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</text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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 encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
clrscrn Clears the screen	auto show statistics	show connection statistics
Olodio tilo oolooni	1	

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (config-host:12) 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.
write host 13 (tunnel-connect-host:16:13) level commands	Stores the current configuration in permanent memory.
- 12	Sets the remote host to establish tunneling connections with.
host 13 (tunnel-connect-host:16:13) 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>
host 13 (tunnel-connect-host:16:13) 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.</text>
host 13 (tunnel-connect-host:16:13) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-</text>
host 13 (tunnel-connect-host:16:13) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.</text>
host 13 (tunnel-connect-host:16:13) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
host 13 (tunnel-connect-host:16:13) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.

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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vih aisanie	makes commediate doing the opening ridarece.
vip enable	Makes connections using the VIP name.
-	
vip enable	Makes connections using the VIP name.
vip enable vip name <text></text>	Makes connections using the VIP name.  Sets the VIP name.
vip enable vip name <text> write</text>	Makes connections using the VIP name.  Sets the VIP name.
vip enable vip name <text> write host 13 (tunnel-connect-host:14:13) level commands</text>	Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
vip enable vip name <text> write host 13 (tunnel-connect-host:14:13) level commands address <text></text></text>	Makes connections using the VIP name.  Sets the VIP name.  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</text>
vip enable vip name <text> write host 13 (tunnel-connect-host:14:13) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></text></text>	Makes connections using the VIP name.  Sets the VIP name.  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</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:13:13) level command	ds .
address <text></text>	Sets the remote host to establish tunneling connections with.
	<pre><text> = IP address or host name of the remote host.</text></pre>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling.
· 	<number> = number of the port to use.</number>

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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
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>	Sets the connect tunnel AES decrypt key 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:11:13) level co	
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:10:13) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
and degraph key shovedesimely	<text> = IP address or host name of the remote host. Sets the connect tunnel AES deprot key with up to 16</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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-

validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the vIP name.  Sotores the current configuration in permanent memory.  host 13 (tunnel-connect-host:9:13) level commands  address < lext>  Sots the remote host to establish tunneling connections with. <a "12="" 12="" 12,3a,bc="" 12.3a.bc="" 123abc="" 12:3a:bc="" 16="" 3a="" a="" adjacent="" aes="" bc"="" be="" by="" byte="" bytes="" bytes.="" certificate="" certificates="" character.="" clears="" client.="" connect="" contains="" decrypt="" digits.="" dsa="" each="" enclose="" encrypt="" for="" hex="" href="https://doi.org/10.1001/j.com/doi.org/10.10&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;ing.&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;wip name &lt;fext&gt;  Sets the VIP name.  Softs the remote host to establish tunneling connections with.&lt;/td&gt;&lt;td&gt;validate certificate enable&lt;/td&gt;&lt;td&gt;Requires verification of the server certificate when con-&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;write stexts Stores the current configuration in permanent memory.  Stores the current configuration in permanent memory.  Stores the current configuration in permanent memory.  Stepts the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.  Learn byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC 12.3A BC 12.3A,BC 12.&lt;/td&gt;&lt;td&gt;vip disable&lt;/td&gt;&lt;td&gt;Makes connections using the specified Address.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;write    Stores the current configuration in permanent memory.   Nost 13 (tunnel-connect-host-9:13) level commands    &lt;/td&gt;&lt;td&gt;vip enable&lt;/td&gt;&lt;td&gt;Makes connections using the VIP name.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  Sets the remote host to establish tunnelling connections with.   stext&gt; = 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 " if="" is="" it="" key="" key.="" may="" must="" name="" note="" optional="" or="" punctuation:="" quotes="" removes="" represented="" rsa="" run="" selection.="" separated="" set="" sets="" single="" spaces.="" ssl="" td="" that="" the="" to="" together="" tunnel="" two="" up="" value="" with=""  =""  <=""><td>vip name <text></text></td><td>Sets the VIP name.</td></a>	vip name <text></text>	Sets the VIP name.
address <rext>  Sets the remote host to establish tunneling connections with. </rext>	write	Stores the current configuration in permanent memory.
with.	host 13 (tunnel-connect-host:9:13) 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.  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.  Sets the connect tunnel AES encrypt key 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.  Sets the connect tunnel AES encrypt key note that quotes must enclose the value if it contains spaces.  Each byte is represented by a single character.  Sets the connect tunnel AES encrypt key.  Removes the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host add</text>	address <text></text>	with.
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 connection statistics  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit to the next higher level.  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 remote port used to establish tunnel connections.	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by 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.  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  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".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.</text></text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Removes the remote port used to establish tunnel connections.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnections.	auto show statistics	show connection statistics
client.  default protocol  default trop keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.	credentials <text></text>	·
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.	default protocol	Restores the default protocol as "TCP".
no address  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 remote port used to establish tunnel connections.	default tcp keep alive	
neling connections.  no aes decrypt key 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 remote port used to establish tunnel connections.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no port Removes the remote port used to establish tunnel connections.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.	no credentials	Clears the RSA/DSA certificate selection.
no ssh username Removes the SSH user name.	no port	
	no ssh username	Removes the SSH user name.

Disables the second TOD been alice times at
Disables the connect mode TCP keep alive timeout.
Removes the VIP name.
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.
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>
Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
Skips verification of the server certificate when connecting.
Requires verification of the server certificate when connecting.
Makes connections using the specified Address.
Makes connections using the VIP name.
Sets the VIP name.
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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.

	<milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:7:13) level commands	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></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.
	Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.
clrscrn	Selects the RSA/DSA certificates by name for the SSL
clrscrn credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
clrscrn credentials <text> default protocol</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep
clrscrn credentials <text>  default protocol default tcp keep alive</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.
clrscrn credentials <text>  default protocol default tcp keep alive exit</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tun-
clrscrn credentials <text>  default protocol default tcp keep alive exit no address</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.
clrscrn credentials <text>  default protocol default tcp keep alive  exit no address no aes decrypt key</text>	Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.

	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:6:13) 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 <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>  aes encrypt key text <text></text></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 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>

tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:5:13) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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.
<del></del>	

no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel con-
	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:4:13) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun-

	neling connections with other devices.
	<text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:3:13) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:2:13) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:1:13) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.

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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (config-host:13) 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 remote port	default value, which depends on the selected protocol.
exit	default value,

clears the name of the host.		
Clears the remote address of the host.	name <text></text>	
Clears the SSH username associated with the host.	no name	Clears the name of the host.
protocol ssh  Sets the protocol to SSH.  Sets the protocol to Telnet.  Sets the IP address of the remote host to connect to wher this host is selected on the login connect menu.    sets the IP address of the remote host to connect to wher this host is selected on the login connect menu.   sets the IP address.   remote port <number> Sets the remote port used to connect to the host. <number> = port to be used.    show Displays the current configuration.   Show history Displays the last 20 commands entered during the current configuration.   Sets the username for logging into the host via SSH.   <tabl< td=""><td>no remote address</td><td>Clears the remote address of the host.</td></tabl<></number></number>	no remote address	Clears the remote address of the host.
protocol telnet  Sets the protocol to Telnet.  Sets the IP address of the remote host to connect to where this host is selected on the login connect menu. <text> = IP address.  Sets the remote port vert of the host.  **connect menu*  **cext&gt; = IP address.  Sets the remote port used to connect to the host.  **cnumber&gt; = port to be used.  Show  Displays the last 20 commands entered during the current CLI session.  Sets the username for logging into the host via SSH.  <text> = Username.  Stores the current configuration in permanent memory.  **host 14 (tunnel-connect-host:16:14) level commands  **address <text></text></text></text>	no ssh username	Clears the SSH username associated with the host.
Sets the IP address of the remote host to connect to wher this host is selected on the login connect menu.    remote port <number>   sets the remote port used to connect to the host.   show Displays the current configuration.   show history Displays the last 20 commands entered during the current CLI session.   sh username <text> Sets the username for logging into the host via SSH.   ctext&gt; = username. stext he username for logging into the host via SSH.   vitte Stores the current configuration in permanent memory.   host 14 (tunnel-connect-host-16:14) level commands   address <text> Sets the remote host to establish tunneling connections with.   vitext&gt; = IP address or host name of the remote host.   aes decrypt key <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 encrypt key <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.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Each byte is represented by two adjacent hex digits.   Bytes may run together or be separated by optional punctuation:   <t< td=""><td>protocol ssh</td><td>Sets the protocol to SSH.</td></t<></hexadecimal></hexadecimal></text></text></number>	protocol ssh	Sets the protocol to SSH.
this host is selected on the login connect menu.    Itemote port < number>   Sets the remote port used to connect to the host.	protocol telnet	Sets the protocol to Telnet.
chumber> = port to be used.   show   Displays the current configuration.	remote address <text></text>	selected on the login connect menu.
Show history  Displays the last 20 commands entered during the current CLI session.  Sets the username for logging into the host via SSH.	remote port <number></number>	
Sets the username <a href="text">text</a> Sets the username for logging into the host via SSH. <a href="text">text</a> Sets the username.  Write Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:16:14) level commands  address <a href="text">text</a> Sets the remote host to establish tunneling connections with. <a href="text">text</a> Sets the connect tunnel AES decrypt key with up to 16 bytes. Seach byte is represented by 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.  aes decrypt key text <a href="text">text</a> Sets the connect tunnel AES decrypt key 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 charact	show	Displays the current configuration.
write Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:16:14) level commands address  Sets the remote host to establish tunneling connections with.	show history	Displays the last 20 commands entered during the current CLI session.
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 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.  Sets the connect tunnel AES encrypt key 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 mus</text></text>	ssh username <text></text>	35 5
Sets the remote host to establish tunneling connections with.    Actext = IP address or host name of the remote host.	write	Stores the current configuration in permanent memory.
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.  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.</text>	host 14 (tunnel-connect-host:16:14) level comn	nands
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.	address <text></text>	with.
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.</text>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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  Clears the screen.  Cedentials <text>  Selects the RSA/DSA certificates by name for the SSL client.</text></text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.</text>	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
clrscrn  Clears the screen.  credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.</text>	auto show statistics	show connection statistics
client.	clrscrn	Clears the screen.
default protocol Restores the default protocol as "TCP".	credentials <text></text>	
	default protocol	Restores the default protocol as "TCP".

default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:15:14) level o	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.

protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	neling connections.  Removes the connect tunnel AES decrypt key.
no address	Removes the remote host address used to establish tun-
exit	alive timeout.  Exits to the next higher level.
default tcp keep alive	Restores the default 45 second connect mode TCP keep
default protocol	Restores the default protocol as "TCP".
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
clrscrn	Clears the screen.
auto show statistics	show connection statistics
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.
	123ABC "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 <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:
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.
	Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

show Shows the current configuration.	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show history  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. <a 12,3a,bc="" 12:3a:bc="" <hexadecimal="" aes="" contains="" enclose="" encrypt="" href="citation-left-square-right-sq&lt;/td&gt;&lt;td&gt;show&lt;/td&gt;&lt;td&gt;-&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Sets the SSH user name for use when establishing tunneling connections with other devices.    top keep alive &lt; milliseconds&gt;&lt;/td&gt;&lt;td&gt;show history&lt;/td&gt;&lt;td&gt;Displays the last 20 commands entered during the current&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  neling connections with other devices.    &lt;/td&gt;&lt;td&gt;show statistics&lt;/td&gt;&lt;td&gt;show connection statistics&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;sets the timer. &lt;/td&gt;&lt;td&gt;ssh username &lt;text&gt;&lt;/td&gt;&lt;td&gt;neling connections with other devices.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  reg.   requires verification of the server certificate when connecting.    &lt;/td&gt;&lt;td&gt;tcp keep alive &lt;milliseconds&gt;&lt;/td&gt;&lt;td&gt;sets the timer.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;necting.  Makes connections using the specified Address.  Wip enable  wip name &lt;text&gt; Sets the VIP name.  write  Stores the current configuration in permanent memory.  Nost 14 (tunnel-connect-host:14:14) level commands  address &lt;text&gt; Sets the remote host to establish tunneling connections with.  &lt;text&gt; = 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 " if="" it="" key="" must="" note="" quotes="" spaces.="" that="" the="" value="">  Sets the connect tunnel AES decrypt key 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 optional punctuation:  123ABC "12,3A,BC 12,3a,bC 12,3a,bC</a>	validate certificate disable	I. ·
vip enable       Makes connections using the VIP name.         vip name <text>       Sets the VIP name.         write       Stores the current configuration in permanent memory.         host 14 (tunnel-connect-host:14:14) level commands         address <text>       Sets the remote host to establish tunneling connections with.         death of the remote host.       Sets the connect tunnel AES decrypt key with up to 16 bytes.         aes decrypt key <hexadecimal>       Sets the connect tunnel AES decrypt key with up to 16 bytes.         aes decrypt key text <text>       Sets the connect tunnel AES decrypt key with up to 16 bytes.         aes decrypt key text <text>       Sets the connect tunnel AES decrypt key with up to 16 bytes.         aes encrypt key <hexadecimal>       Sets the connect tunnel AES encrypt key with up to 16 bytes.         aes encrypt key <hexadecimal>       Sets the connect tunnel AES encrypt key with up to 16 bytes.         aes hyte is represented by two adjacent hex digits.       Bytes may run together or be separated by optional punctuation:         123ABC *12 3A BC* *12,3A,BC *12.3a,bc *12.3a,b</hexadecimal></hexadecimal></text></text></hexadecimal></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  write Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:14:14) level commands  address <text> Sets the remote host to establish tunneling connections with.</text></text>	vip disable	Makes connections using the specified Address.
write Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:14:14) 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.  aes encrypt key &lt; hexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.</text>	vip enable	Makes connections using the VIP name.
Sets the remote host to establish tunneling connections with.	vip name <text></text>	Sets the VIP name.
address <text>  Sets the remote host to establish tunneling connections with.  <text>= IP address or host name of the remote host.  aes decrypt key <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 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.</hexadecimal></text></text>	write	Stores the current configuration in permanent memory.
with. <text> = IP address or host name of the remote host.  aes decrypt key <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>  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Sets the connect tunnel AES encrypt key 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.</text></hexadecimal></text></hexadecimal></text>	host 14 (tunnel-connect-host:14:14) level commands	
bytes. Each byte is represented by 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.  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>  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics  Clears the screen.</text></hexadecimal></text>	address <text></text>	with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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  clrscrn  Clears the screen.</text></hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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  clrscrn  Clears the screen.</text>	aes decrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
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.	aes encrypt key <i><hexadecimal></hexadecimal></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
clrscrn Clears the screen.	aes encrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
	auto show statistics	show connection statistics
credentials <text> Selects the RSA/DSA certificates by name for the SSL</text>	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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.

Sets the connect tunnel AES decrypt key with 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*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 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*1		<text> = IP address or host name of the remote host.</text>
bytes. Each byte is represented by 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.  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.  Sets the connect tunnel AES encrypt key 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.  Clears the screen.  Getars the screen.  Gedentials <text> Glears the screen.  Gedentials <text> Glears the screen.  Gedentials <text> Glears the screen.  Gedentials <text> Getars the screen.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Removes the remote port used to establish tunneling one 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</text></text></text></text></text>	aes decrypt kev <hexadecimal></hexadecimal>	
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 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. Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the enveloped to set destablish tunneling connections.  No address  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 use for connect mode tunneling.  Protocol tsp  Protocol tcp  Uses TCP protocol for connect mode		bytes.
tuation: 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 '123A 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 connection statistics  Clears the screen.  Clears the screen.  Clears the screen.  Credentials <table by="" of="" service="" t<="" td="" the=""><td></td><td></td></table>		
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* 12,3ABC* 12,3ABC* 12,3ABC* 12,3aBC* 123abc* 123abc* 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* 12,3aB		
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 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. 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.  Citizen (Citizens the screen.)  Citizens the screen.  Citizens the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default trotocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  no ase decrypt key  Removes the connect tunnel AES decrypt key.  no credentials  Citizens the RSA/DSA certificate selection.  Removes the remote port used to establish tunneling connections.  no sh username  No top keep alive  Disables the connect tunnel AES encrypt key.  Citizens 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 VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SCH protocol for connect mode tunneling.  Uses TCP protocol for connect mode tunneling.		
Sets the connect tunnel AES decrypt key 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 statistics christians and the space of the value if it contains spaces.  Sets the connection statistics clirscrn  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".  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Removes the default for the post diversion of the stablish tunneling connections.  No address  Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES decrypt key. Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunneling connections.  Removes the PSA/DSA certificate selection.  Removes the RSA/DSA certificate selection.  Removes the SH user name.  Disables the connect mode TCP keep alive timeout.  Removes the SH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol sch Uses SCH protocol for connect mode tunneling.  Uses SCH protocol for connect mode tunneling.  Uses TCP protocol for c		· ·
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 1	aes decrypt key text <text></text>	·
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: 123/ABC "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 screen.  Clears the screen.  Credentials <iext> Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  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 remote port used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  No sish username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rumber&gt;  In unimber&gt;  Removes TCP protocol for connect mode tunneling.  Protocol tsp  Uses SSL protocol for connect mode tunneling.</iext>	, ,	bytes.
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 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.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  no address Removes the remote host address used to establish tunneling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no credentials Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunneling connections.  no sph username Removes the remote port 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 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 to establish tunnel connections.  No sph username Removes the remote port used to establish tunnel connections.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh Uses SSL protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.		
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.  Show connection statistics cirscm 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".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the default 45 second connect mode TCP keep alive timeout.  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 remote port used to establish tunneling confections.  Removes the remote port used to establish tunnel connections.  Removes the FSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Sets the RSA/DSA certificate selection.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <a href="https://www.number&gt;">www.number&gt;</a> enumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  Protocol ssh Uses TCP protocol for connect mode tunneling.		· ·
Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  123ABC "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 cirscm Clears the screen.  Credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  Exist to the next higher level.  Removes the connect tunnel AES decrypt key.  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 tunnections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the sSH user name.  Removes the SSH user name.  Sets the remote port used to establish tunnel connections.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Sets the remote port to use.  Protocol ssh Uses SSH protocol for connect mode tunneling.  Protocol top  Uses TCP protocol with AES encryption for connect mode</text></text>	aes encrypt key <hexadecimal></hexadecimal>	
Bytes may run together or be separated by optional punctuation:  123ABC "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  cirsorn  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  no address  Removes the connect tunnel AES decrypt key. Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.  Removes the remote port used to establish tunneling confections.  no port  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 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 to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  vnumber&gt; Sets the remote port to use for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Protocol ssl  Uses SSL protocol for connect mode tunneling.  Protocol tcp  Uses TCP protocol with AES encryption for connect mode  Uses TCP protocol with AES encryption for connect mode  Uses TCP protocol with AES encryption for connect mode</text>		
tuation: 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.  auto show statistics  show connection statistics  cirscrn  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".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no aed decrypt key  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 certificates election.  Removes the remote port used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the connect tunnel AES encrypt key.  Sets the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SSL protocol for connect mode tunneling.  Protocol ssl  Uses SSL protocol for connect mode tunneling.  Protocol tcp  Uses TCP protocol with AES encryption for connect mode		
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  cliescrn  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  exit  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  no aes decrypt key  no aes encrypt key  Removes the connect tunnel AES decrypt key.  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel on-nections.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the connect tunnel AES encrypt key.  Clears the default 45 second connect tunnel AES encrypt key.  Disables the connect tunnel AES encrypt key.  Sets the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  No vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SSL protocol for connect mode tunneling.  Protocol ssl  Uses SSL protocol for connect mode tunneling.  Protocol tcp  Uses TCP protocol with AES encryption for connect mode</text>		tuation:
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  Clears the screen.  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 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  runmber&gt;  Protocol ssh Uses SSL protocol for connect mode tunneling.  Uses SCL protocol with AES encryption for connect mode</text>		
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.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel or nections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh Uses SSH protocol for connect mode tunneling.  Protocol tcp Uses TCP protocol with AES encryption for connect mode		·
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.  Clears the screen.  Credentials   Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  romber> enumber> enumber of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.  Protocol tsp  Uses TCP protocol with AES encryption for connect mode	aes encrypt key text <text></text>	
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".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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 SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no trumber> enumber to the port to use.  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSL protocol for connect mode tunneling.  Uses TCP protocol with AES encryption for connect mode		1.3
auto show statistics clrscm Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address 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 remote port used to establish tunnel or 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 remote port used to establish tunnel connections.  Removes the VIP name.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Uses SSL protocol for connect mode tunneling.  protocol tsp Uses TCP protocol with AES encryption for connect mode		
credentials <text>  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel or nections.  Removes the remote port used to establish tunnel or nections.  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 SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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</number></text>		· ·
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel or nections.  Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol with AES encryption for connect mode	auto show statistics	show connection statistics
client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol with AES encryption for connect mode	clrscrn	
Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roundber> = 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	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = 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	default protocol	Restores the default protocol as "TCP".
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 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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  protocol ssl  Uses SSL protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol with AES encryption for connect mode	default tcp keep alive	
neling connections.  no aes decrypt key  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  protocol ssl  Uses SSL protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol with AES encryption for connect mode	exit	Exits to the next higher level.
no aes encrypt 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 SSH user name.  Removes the VIP name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = 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	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  cnumber> = number of the port to use.  protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Uses TCP protocol with AES encryption for connect mode	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = 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  Uses TCP protocol with AES encryption for connect mode	no aes encrypt key	Removes the connect tunnel AES encrypt key.
no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Removes the vIP name.  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  Uses TCP protocol with AES encryption for connect mode	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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  Uses TCP protocol with AES encryption for connect mode</number>	no port	·
no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre> 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	no ssh username	Removes the SSH user name.
port <number> 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.  Uses TCP protocol with AES encryption for connect mode</number></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
<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. Uses TCP protocol with AES encryption for connect mode</number>	no vip name	Removes the VIP name.
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	port < <i>number</i> >	
protocol tcp Uses TCP protocol for connect mode tunneling. protocol tcp aes Uses TCP protocol with AES encryption for connect mode	protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol tcp aes  Uses TCP protocol with AES encryption for connect mode	protocol ssl	Uses SSL protocol for connect mode tunneling.
	protocol tcp	Uses TCP protocol for connect mode tunneling.
	protocol tcp aes	

protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:12:14) level commands	J
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

with.	host 14 (tunnel-connect-host:11:14) 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 '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 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 optional punctuation:  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.  Clears the screen.  Clears the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default the second connect mode TCP keep alive timeout.  Exists to the next higher level.  Part of the protocol as "TCP".  Removes the remote host address used to establish tunneling connections.  No ass encrypt key  Removes the connect tunnel AES encrypt key.  Removes the connect nunel AES encry	address <text></text>	_
bytes. 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 ABC *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 optional punctuation: 123ABC *12.3a BC* *12.3a,BC* *12		<text> = IP address or host name of the remote host.</text>
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 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.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  no aes encrypt key Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES decrypt key.  Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  No top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode tunneling.  Protocol ssh  Uses SSH protocol for connect mode tunneling.</hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key. Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel or nections.  Removes the remote port used to establish tunnel or nections.  Removes the remote port used to establish tunnel or nections.  Removes the sconnect tunnel AES encrypt key.  Removes the remote port used to establish tunnel connections.  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Remover a mumber> sets the remote port to use for connect mode tunneling.  Removers the VIP name.  Sets the remote port to use for connect mode tunneling.	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no port  Removes the SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  - number = number of the port to use.  Uses SSH protocol for connect mode tunneling.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel or rections.  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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <ul> <li>Aumber&gt;</li> <li>Sets the remote port to use.</li> <li>Uses SSH protocol for connect mode tunneling.</li> <li>Uses SSL protocol for connect mode tunneling.</li> </ul>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 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 SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Anumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	auto show statistics	show connection statistics
default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 port used to establish tunneling to establish tunneling connections.  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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  In alive timeout.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  In alive timeout.  In alive timeou	default protocol	Restores the default protocol as "TCP".
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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  enumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	default tcp keep alive	
neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	exit	Exits to the next higher level.
Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 address	
Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  Protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no top keep alive  Removes the VIP name.  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.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Removes the VIP name.  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.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	no port	· ·
no vip name  Removes the VIP name.  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 ssh username	Removes the SSH user name.
port <number> 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></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
<pre>conumber = number of the port to use.</pre> protocol ssh Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.	no vip name	Removes the VIP name.
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	Uses SSL protocol for connect mode tunneling.
	protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol top aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol udp  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp aes  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  show  Show is the current configuration.  Displays the last 20 commands entered during the current configuration and tunneling.  Show statistics  show connection statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.  state > SSH user name for use when establishing tunneling connections with other devices.  state > SSH user name.  top keep alive < milliseconds>  estate to time.  «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.  Validate certificate enable  Requires 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.  Validate certificate enable  Requires 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.  Validate certificate enable  Requires 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 VIP name.  Vip name   Validate certificate when connecting the VIP name.  Validate certificate when connecting the VIP name.  Validate certificate when connecting the VIP name.  Validate Certific		
ing.  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Show Show with current configuration.  Show 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.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect unde tunneling 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.  Makes connections using the specified Address.  vip disable  vip name   Makes connections using the VIP name.  vip name   Sets the VIP name.  Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host-10:14) level commands  address   Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3AB C*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 optional punctuation:  123ABC*12 3AB 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 encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC*12 3AB C*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</milliseconds>	protocol tcp aes	
protocol udp aes  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  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  **cmilliseconds&gt; = timer value, in milliseconds.  Validate certificate disable  Skips verification of the server certificate when connecting.  Vip disable  Vip disable  Wakes connections using the specified Address.  Vip enable  Makes connections using the specified Address.  Vip aname &lt;*/td&gt;  **Requires verification of the server certificate when connecting.  Vip enable  Makes connections using the specified Address.  Vip name &lt;*/td&gt;  **Requires verification of the server certificate when connecting.  Vip enable  Makes connections using the specified Address.  Vip name &lt;*/td&gt;  **Requires verification of the server certificate when connecting.  Vip enable  Makes connections using the specified Address.  Vip enable  Nakes connections using the specified Address.  Vip name &lt;*/td&gt;  **Requires verification of the server certificate when connecting.  Vip disable  Vip name &lt;*/td&gt;  **Requires verification of the server certificate when connecting.  Vip disable  Vip enable  Nakes connections using the specified Address.  Vip enable  Sets the Current configuration in permanent memory.  Note: 14 (tunnel-connect-host:10:14) level commands  **Requires verification of the server certificate when connections with.  **Learne **Itale **Allower **Itale **Allower **Itale **It</milliseconds>	protocol telnet	I.
tunneling.	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.  - dext> = SSH user name.  tcp keep alive <milliseconds></milliseconds>	protocol udp aes	
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices.  tcp keep alive <milliseconds>  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  <milliseconds> et mer value, in milliseconds.  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the specified Address.  Vip name <text>  Sets the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:10:14) 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 optional punctuation:  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 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.</text></text></text></text></milliseconds></milliseconds></milliseconds>	show history	
nelling connections   with other devices.   etaxl= SSH user name.	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Note 14 (tunnel-connect-host:10:14) 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.  3es encrypt key &lt; hexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Write  Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:10:14) 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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate disable	I. ·
vip enable  vip name <text> Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 14 (tunnel-connect-host:10:14) 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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  host 14 (tunnel-connect-host:10:14) 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 optional punctuation: 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Stes the current current permanent memory.   Stes the current current current permanent memory.   Stes the current current permanent memory.   Stes the current current current permanent memory.   Stes the current current current permanent memory.   Stes the current current	vip enable	Makes connections using the VIP name.
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 optional punctuation: 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vip name <text></text>	Sets the VIP name.
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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>		
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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	write	Stores the current configuration in permanent memory.
aes decrypt key <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.  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</hexadecimal>	- 12	Stores the current configuration in permanent memory.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	host 14 (tunnel-connect-host:10:14) level commands	Sets the remote host to establish tunneling connections with.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	host 14 (tunnel-connect-host:10:14) level commands	Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	host 14 (tunnel-connect-host:10:14) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	host 14 (tunnel-connect-host:10:14) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	host 14 (tunnel-connect-host:10:14) level commands address <text> aes decrypt key <hexadecimal> aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:9:14) level cor	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 < <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
protocol ssh	Uses SSH protocol for connect mode tunneling.
·	1

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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:8:14) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

wip name <a href="mailto:right: 2015">wip name <a href="mailto:right: 2015">wip name <a href="mailto:right: 2015">xip name <a "12="" 12="" 12,3a,bc="" 12.3a.bc="" 123="" 16="" 3a="" <fext="" a="" abc="" adjacent="" aes="" bc"="" be="" by="" byte="" bytes="" bytes.="" character.="" clears="" connect="" contains="" credentials="" decrypt="" digits.="" each="" enclose="" encrypt="" hex="" href="mailto:right:&lt;/th&gt;&lt;th&gt;vip disable&lt;/th&gt;&lt;th&gt;Makes connections using the specified Address.&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;write write write write write states of the VIP name.  Stores the VIP name.  Stores the current configuration in permanent memory.  Nest 14 (tunnel-connect-host:7:14) level commands address &lt; lext&gt;  Sets the remote host to establish tunneling connections with.  ⟨ext&gt;   P address or host name of the remote host.  aes decrypt key &lt; hexadecimal&gt;  Sets the remote host to establish tunneling connections with.  ⟨ext&gt;   P address or host name of the remote host.  aes decrypt key kex &lt; lext&gt;  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex 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&lt;/td&gt;&lt;td&gt;&lt;u&gt;                                     &lt;/u&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  Sets the remote host to establish tunneling connections with.                                      &lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  Sets the remote host to establish tunneling connections with.                                      &lt;/td&gt;&lt;td&gt;write&lt;/td&gt;&lt;td&gt;Stores the current configuration in permanent memory.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;with.    stext = IP address or host name of the remote host.   aes decrypt key &lt; hexadecimal&gt;    &lt;/td&gt;&lt;td&gt;host 14 (tunnel-connect-host:7:14) level commands&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123/ABC " if="" is="" it="" key="" may="" must="" note="" optional="" or="" punctuation:="" quotes="" represented="" run="" screen.="" separated="" sets="" single="" spaces.="" that="" the="" to="" together="" tunnel="" two="" up="" value="" with=""> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive  exit Exits to the next higher level.  no address Removes the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no credentials Clears the RSA/DSA certificate selection.  Removes the remote host address used to establish tunneling connections.  no set user tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no set user mane.  Disables the connect mode TCP keep alive timeout.<td>address <text></text></td><td>with.</td></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>	address <text></text>	with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 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  clrscrn Clears the screen.  Clears the screen.  Credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive  Exits to the next higher level.  no address Removes the remote host address used to establish tunneling connections.  no aes encrypt key Removes the connect tunnel AES encrypt key.  Removes the connect 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 connect tunnel AES encrypt key.  Removes the RSA/DSA certificate selection.  Removes 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.</text></hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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  cliscrn  Clears the screen.  credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  no aeddress  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.  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 to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text></text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no port Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text>	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
clrscrn  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnections.  no port  Removes the remote port used to establish tunnections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials < text>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	auto show statistics	show connection statistics
default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 connect tunnel AES encrypt key.  Removes the remote port used to establish tunnel 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.  Disables the connect mode TCP keep alive timeout.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 encrypt 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 SSH user name.  Disables the connect mode TCP keep alive timeout.	default protocol	Restores the default protocol as "TCP".
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 encrypt key. Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	default tcp keep alive	
neling connections.  no aes decrypt key 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  no ssh username Removes the SSH user name.  no tcp keep alive Disables the connect mode TCP keep alive timeout.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive Disables the connect mode TCP keep alive timeout.	no port	i i
	no ssh username	Removes the SSH user name.
no vip name Removes the VIP name.	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
	no vip name	Removes the VIP name.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-

validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the vIP name.  Sets the current configuration in permanent memory.  host 1/4 (tunnel-connect-host:5:1/4) level commands  address < lext>  Sets the remote host to establish tunneling connections with.		ing.
wip name <fext>  Sets the VIP name.  Softs the remote host to establish tunneling connections with.</fext>	validate certificate enable	Requires verification of the server certificate when con-
write write Stores the current configuration in permanent memory.  **Note 14 (tunnel-connect-host:5:14) level commands**  **address < text>**  **Sets the remote host to establish tunneling connections with. **  **ctext> = IP address or host name of the remote host.  **Sets the connect tunnel AES decrypt key with up to 16 bytes.  **Bach byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC **12.3A.BC **12	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Nost 14 (tunnel-connect-host-5:14) level commands	vip enable	Makes connections using the VIP name.
Sets the remote host to establish tunnelling connections with.   stext = 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 decrypt key 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.	vip name <text></text>	Sets the VIP name.
address <rext>  Sets the remote host to establish tunneling connections with. </rext>	write	Stores the current configuration in permanent memory.
with.	host 14 (tunnel-connect-host:5:14) 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 "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.  Sets the connect tunnel AES encrypt key 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.  Sets the connect tunnel AES encrypt key note that quotes must enclose the value if it contains spaces.  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 and the protocol of the value if it contains spaces.  Each byte is represented by the protocol of the value if it contains spaces.  Each byte is repr</text>	address <text></text>	with.
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 connection statistics  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit to the next higher level.  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 remote port used to establish tunnel connections.	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by 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.  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  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".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.</text></text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnections.	auto show statistics	show connection statistics
client.  default protocol  default trop keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.	credentials <text></text>	·
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.	default protocol	Restores the default protocol as "TCP".
no address  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 remote port used to establish tunnel connections.	default tcp keep alive	
neling connections.  no aes decrypt key 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 remote port used to establish tunnel connections.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no port Removes the remote port used to establish tunnel connections.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.	no credentials	Clears the RSA/DSA certificate selection.
no ssh username Removes the SSH user name.	no port	
	no ssh username	Removes the SSH user name.

no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:4:14) 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>	Sets the connect tunnel AES encrypt key 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.

	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel con-
	· · · · · · · · · · · · · · · · · · ·

	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:2:14) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:1:14) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (config-host:14) 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. <a href="text"><a 12="" 12,3a,bc="" 12.3a.bc="" 12:3a:bc="" 3a="" bc"="" contains="" enclose="" href="text&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;write&lt;/td&gt;&lt;td&gt;Stores the current configuration in permanent memory.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;host 15 (tunnel-connect-host:16:15) level commands&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;address &lt;text&gt;&lt;/td&gt;&lt;td&gt;Sets the remote host to establish tunneling connections with.  &lt;text&gt; = IP address or host name of the remote host.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;aes decrypt key &lt;hexadecimal&gt;&lt;/td&gt;&lt;td&gt;Sets the connect tunnel AES decrypt key with 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="" must="" note="" quotes="" spaces.<="" td="" that="" the="" value=""></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:15:15) 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

1	Note that quotes must enclose the value if it contains spaces.
b E N	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
b E B tu 1	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 23ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
b E N	Sets the connect tunnel AES encrypt key 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 s	how connection statistics
clrscrn	Clears the screen.
	Selects the RSA/DSA certificates by name for the SSL slient.
default protocol	Restores the default protocol as "TCP".
	Restores the default 45 second connect mode TCP keep live timeout.
exit E	Exits to the next higher level.
	Removes the remote host address used to establish tun- neling 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 C	Clears the RSA/DSA certificate selection.
	Removes the remote port used to establish tunnel con- nections.
no ssh username R	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
	Sets the remote port to use for connect mode tunneling. cnumber> = number of the port to use.
protocol ssh U	Jses SSH protocol for connect mode tunneling.
protocol ssl U	Jses SSL protocol for connect mode tunneling.
protocol tcp U	Jses TCP protocol for connect mode tunneling.
	Jses TCP protocol with AES encryption for connect mode unneling.
l' .	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp U	Jses UDP protocol for connect mode tunneling.
protocol udp aes U	
	Jses UDP protocol with AES encryption for connect mode unneling.

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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:14:15) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:12:15) 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>	Sets the connect tunnel AES encrypt key 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:11:15) level co	
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
aco deciypt ney Alexadecillai>	bytes.
	Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-
	tuation:
	123ABC "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
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16
aco chorypt key text stext?	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.

	I
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:9:15) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

host 15 (tunnel-connect-host:7:15) level commands	6
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 top aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  show  Show the current configuration.  Shows the current configuration.  Displays the last 20 commands entered during the current configuration are commands entered during the current configuration.  Show statistics  show connection statistics  ssh username <a href="#">***/**/**/*//*//////////////////////</a>		
ing.  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  show  Show show the current configuration.  Show show show connection statistics  show connection statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.  Attack = SSH user name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  Amiliseconds&gt;  Enables TCP keep alive for connect mode tunneling and sets the timer.  Amiliseconds&gt; = 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.  Vip disable  Makes connections using the specified Address.  Vip enable  Makes connections using the specified Address.  Vip enable  Makes connections using the specified Address.  Vip enable  Makes connections using the viP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Inost 15 (tunnel-connect-host-6:15) level commands  address &lt; text&gt;  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key 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.  Parks may run together or be separat</milliseconds>	protocol tcp aes	
protocol udp aes  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  show connection statistics  show connections trained for use when establishing tunneling connections with other devices name.  tcp keep alive <a href="mailto:right-qual-tilde">right-qual-tilde</a> tcp keep alive <a href="mailto:right-qual-tilde">right-qual-tilde</a> Enables TCP keep alive for connect mode tunneling and sets the timer.  **Texts = SSH user name.**  tcp keep alive <a href="mailto:right-qual-tilde">right-qual-tilde</a> Packets = SSH user name.  tcp keep alive <a href="mailto:right-qual-tilde">right-qual-tilde</a> **Texts = SSH user name.  tcp keep alive or connect mode tunneling and sets the timer.  **Intilisecondss = timer value, in milliseconds.**  validate certificate disable  Skips verification of the server certificate when connecting.  vip disable  Vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the specified Address.  Vip name <a href="mailto:right-qual-tilde">right-qual-tilde</a> **Requires verification of the server certificate when connecting.  Vip disable  Vip name <a href="mailto:right-qual-tilde">right-qual-tilde</a> Makes connections using the specified Address.  Vip name <a href="mailto:right-qual-tilde">right-qual-tilde</a> **Requires verification of the server certificate when connecting.  Vip disable  Vip name <a href="mailto:right-qual-tilde">right-qual-tilde</a> **Requires verification of the server certificate when connecting.  Vip disable  Vip name <a href="mailto:right-qual-tilde">right-qual-tilde</a> **Requires verification of the server certificate when connecting.  Vip disable  Vip name <a href="mailto:right-qual-tilde">right-qual-tilde</a> **Requires verification of the server certificate when connecting.  Vip disable  Vip name <a "12="" 12="" 12,3a="" 12,3a,bc="" 12.3a="" 123abc="" 12:3a="" 16="" 3a="" adjacent="" aes="" bc="" bc"="" be="" by="" byte="" bytes="" bytes.="" connect="" contains="" digits.="" each="" enclose="" encrypt="" hex="" href="mailto:right-&lt;/td&gt;&lt;td&gt;protocol telnet&lt;/td&gt;&lt;td&gt;I.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  tunneling.    &lt;/td&gt;&lt;td&gt;protocol udp&lt;/td&gt;&lt;td&gt;Uses UDP protocol for connect mode tunneling.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;show history  Displays the last 20 commands entered during the current CLI session.  show statistics  sh username &lt;text&gt;  Sets the SSH user name for use when establishing tunneling connections with other devices. &lt;text&gt; = SSH user name for use when establishing tunneling connections with other devices. &lt;text&gt; = SSH user name.  tcp keep alive &lt;milliseconds&gt;  Enables TCP keep alive for connect mode tunneling and sets the timer.  validate certificate disable  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name &lt;text&gt;  sets the VIP name.  Stores the current configuration in permanent memory.  host 15 (tunnel-connect-host:6:15) level commands  address &lt;text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = 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.  aes encrypt key &lt;hexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex 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.  aes encrypt key &lt;hexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  123.4BC 12.3A BC 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 encrypt key with up to 16 bytes.  Each byte is represented b&lt;/td&gt;&lt;td&gt;protocol udp aes&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  CLI session.    &lt;/td&gt;&lt;td&gt;show&lt;/td&gt;&lt;td&gt;Shows the current configuration.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Sets the SSH user name for use when establishing tunneling connections with other devices.  tcp keep alive &lt;milliseconds&gt;  tcp keep alive &lt;milliseconds&gt;  Enables TCP keep alive for connect mode tunneling and sets the timer.  &lt;milliseconds&gt; = timer value, in milliseconds.  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the specified Address.  vip name &lt;text&gt; Sets the VIP name.  vip name &lt;text&gt; Sets the VIP name.  **Stores the current configuration in permanent memory.  **Nost 15 (tunnel-connect-host-6:13) level commands*  address &lt;text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Bach byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC " if="" is="" it="" key="" may="" must="" note="" optional="" or="" punctuation:="" quotes="" represented="" run="" separated="" sets="" spaces.="" spaces.<="" td="" that="" the="" to="" together="" tunnel="" two="" up="" value="" with=""><td>show history</td><td></td></a>	show history	
neling connections with other devices.  tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip name <text> Sets the VIP name.   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.   address <text> Sets the connect tunnel AES decrypt key with up to 16 bytes.   aes decrypt key <hexadecimal> Sets the connect tunnel AES decrypt key with up to 16 bytes.   aes decrypt key text <lext> Sets the connect tunnel AES decrypt key with up to 16 bytes.   aes hybe is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  123ABC "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 <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.</text></hexadecimal></lext></hexadecimal></text></text></milliseconds></milliseconds>	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Nost 15 (funnel-connect-host:\$:15) 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.  aes decrypt key &lt;*hexadecimal&gt;**  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 15 (tunnel-connect-host:6:15) 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.  aes encrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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 two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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.</hexadecimal></text></text></text>	validate certificate disable	l. '
vip enable  vip name <text> Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 15 (tunnel-connect-host:6:15) 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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 15 (tunnel-connect-host:6:15) 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Nost 15 (tunnel-connect-host:6:15) level commands	vip enable	Makes connections using the VIP name.
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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vip name <text></text>	Sets the VIP name.
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 optional punctuation: 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.</text>	The state of the s	
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.</text>	-	Stores the current configuration in permanent memory.
aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></hexadecimal>	write	Stores the current configuration in permanent memory.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES encrypt key with up to 16 bytes.  5 Sets the connect tunnel AES encrypt key with up to 16 bytes.  5 Sets the connect tunnel AES encrypt key with up to 16 bytes.	write host 15 (tunnel-connect-host:6:15) level commands	Sets the remote host to establish tunneling connections with.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	write host 15 (tunnel-connect-host:6:15) 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>
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	write host 15 (tunnel-connect-host:6:15) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	write host 15 (tunnel-connect-host:6:15) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	write host 15 (tunnel-connect-host:6:15) level commands address <text> aes decrypt key <hexadecimal> aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:5:15) 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 <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>	Sets the connect tunnel AES encrypt key 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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> tcp keep alive <milliseconds></milliseconds></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and</text>
top keep diive aminiseeonas	sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:3:15) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:2:15) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-

	ing.
validate certificate enable	Requires verification of the server certificate when con-
validate certificate eriable	necting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:1:15) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
	<pre><text> = IP address or host name of the remote host.</text></pre>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.

tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  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  show connection statistics  show connections statistics  state the SSH user name for use when establishing tunneling connections with other devices.    top keep alive <milliseconds>   top keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name &lt;<a href="mailto:kext">kerts VIP name</a>  sets the VIP name.  Stores the current configuration in permanent memory.  <b>Instit 5 (config-host:15) level commands</b>  cliscon  Clears the screen.  Gefault protocol  default protocol  default protocol  default protocol  default protocol  cexit  Exits to the configuration level.  Change to config host level  name &lt;<a href="mailto:kext">keep level  name &lt;<a href="mailto:keepeds">keepeds</a>  Sets the name of the host.  <a href="mailto:keepeds">keepeds</a>  clears the name of the host.  clears the name of the host.  clears the screen.  Glears the screen.  Glears the screen.  Clears the screen.  Clears the screen.  Sets the name of the host.  clears the same and the host.  clears the screen and of the host.  clears t</a></milliseconds></milliseconds></milliseconds>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
cumbers = number of the port to use.		·
protocol test pr	port <number></number>	
protocol tcp ass Uses TCP protocol for connect mode tunneling.  protocol tcp ass Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet Uses TDP protocol (with IAC) for connect mode tunneling.  protocol udp Uses UDP protocol for connect mode tunneling.  protocol udp ass 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.    Sets the SSH user name for use when establishing tunneling connections with other devices.	protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol tep aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Show  Shows the current configuration.  Show show is the sat 20 commands entered during the current CLI session.  Show statistics  Show connection statistics  Show connection statistics  Show connection statistics  Show connection statistics  Show is self user name for use when establishing tunneling connections.  Sets the SSH user name for use when establishing tunneling connections.  With other devices.  **c+ox** = SSH user name.  **tep AEM = AEM	protocol ssl	Uses SSL protocol for connect mode tunneling.
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  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  show connection statistics  show connections statistics  state the SSH user name for use when establishing tunneling connections with other devices.    top keep alive <milliseconds>   top keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name &lt;<a href="mailto:kext">kerts VIP name</a>  sets the VIP name.  Stores the current configuration in permanent memory.  <b>Instit 5 (config-host:15) level commands</b>  cliscon  Clears the screen.  Gefault protocol  default protocol  default protocol  default protocol  default protocol  cexit  Exits to the configuration level.  Change to config host level  name &lt;<a href="mailto:kext">keep level  name &lt;<a href="mailto:keepeds">keepeds</a>  Sets the name of the host.  <a href="mailto:keepeds">keepeds</a>  clears the name of the host.  clears the name of the host.  clears the screen.  Glears the screen.  Glears the screen.  Clears the screen.  Clears the screen.  Sets the name of the host.  clears the same and the host.  clears the screen and of the host.  clears t</a></milliseconds></milliseconds></milliseconds>	protocol tcp	Uses TCP protocol for connect mode tunneling.
ing.    Juse UDP protocol for connect mode tunneling.   Juse UDP protocol with AES encryption for connect mode tunneling.   Show	protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Show the current configuration.  Show history  Displays the last 20 commands entered during the current CLI session.  Show statistics  show connection statistics  show connection statistics  show connection statistics  ssh username <text>  Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.  validate certificate disable  Skips verification of the server certificate when connecting.  vip disable  Wakes connections using the specified Address.  vip enable  Makes connections using the specified Address.  vip name <text>  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  host 15 (config-host:15) level commands  cirsorn  default protocol  Restores the default value of the protocol (Teinet).  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>  Change to config host level  and <iext>  Sets the name of the host.   clears the name of the host.  on name  Clears the semane associated with the host.  Clears the semane associated with the host.  Clears the semane associated with the host.  Sets the protocol to SSH.  Sets the protocol to SSH.</iext></number></text></milliseconds></milliseconds></text></text>	protocol telnet	I
show Shows the current configuration.  show history Displays the last 20 commands entered during the current CLI session.  show statistics Show connection statistics  show statistics Sets the SSH user name for use when establishing tunneling connections with other devices.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the current CLI session.  show connection statistics  ssh username <text>  Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer. <millisecondss <text="" =="" address.="" certificate="" connecting.="" connections="" disable="" enable="" in="" makes="" milliseconds.="" name="" name.="" of="" requires="" server="" skips="" specified="" the="" timer="" using="" validate="" value,="" verification="" vip="" when="">  Sets the VIP name.  Sots the VIP name.  Vip name <text>  Sets the current configuration in permanent memory.  Nost 15 (config-host:15) level commands  clrscrn  Clears the screen.  default protocol  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.  Costs the configuration level.  Costs the name of the host.  <text> = 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 usemame associated with the host.  Protocol ssh  Sets the protocol to Telnet.</text></text></text></millisecondss></milliseconds></text></text>	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
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 for use when establishing tunneling connections with other devices. <text> = SSH user name.   tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip name <text> Sets the VIP name.   write Stores the current configuration in permanent memory.   host 15 (config-host:15) level commands Clears the screen.   default protocol Restores the default value of the protocol (Telnet).   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> Change to config host level   no name Change to config host level   no name Clears the name of the host.   no remote address Clears the name of the host.   no seh username Clears the sernet address of the host.   rotocol seh Sets the protocol to SSH.</number></text></milliseconds></milliseconds></text></text>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip name <text> Sets the VIP name.   write Stores the current configuration in permanent memory.   host 15 (config-host:15) level commands 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> Change to config host level   no name Clears the name of the host.   no remote address Clears the name of the host.   clears the remote address of the host.   no remote address Clears the remote address of the host.   protocol ssh Sets the protocol to Telnet.</number></text></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the current CLI session.
neling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  vite  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  default value, which depends on the selected protocol.  exit  Exits to the configuration level.  host <number>  Change to config host level  sets the name of the host. <text> = name of the host.  clears the name of the host.  Clears the name of the host.  Clears the remote address of the host.  no name  Clears the remote address of the host.  Clears the remote address of the host.  Clears the remote address of the host.  Clears the SSH username associated with the host.  Protocol ssh  Protocol telnet  Sets the protocol to Telnet.</text></number></text></milliseconds></milliseconds></text>	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Wip enable  Makes connections using the VIP name.  Wip name <text> Sets the VIP name.  Wite Stores the current configuration in permanent memory.  **Nost 15 (config-host:15) level commands**  clrscrn  Clears the screen.  default protocol  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>  Change to config host level  name <text> Sets the name of the host.  <text> = name of the host.  To remote address  Clears the screen.  Clears the remote address of the host.  Clears the name associated with the host.  Sets the protocol to SSH.  Sets the protocol to Telnet.</text></text></number></text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
vip disable  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  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>  Change to config host level  name <text>  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.  protocol ssh  Sets the protocol to Telnet.</text></text></number></text>	validate certificate disable	l. ·
vip enable       Makes connections using the VIP name.         vip name < text>       Sets the VIP name.         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>       Change to config host level         name < text>       Sets the name of the host.         ctext> = name of the 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.	validate certificate enable	·
vip name <text> Sets the VIP name.  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.  Change to config host level  name <text>  Sets the name of the host.  <text> = name of the host.  clears the name of the host.  no remote address  Clears the remote address of the host.  Clears the SSH username associated with the host.  protocol ssh  Sets the protocol to Telnet.</text></text></text>	vip disable	Makes connections using the specified Address.
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).  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>  Change to config host level  name <text>  Sets the name of the host. <text> = name of the host.  clears the 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.  protocol ssh  Sets the protocol to Telnet.</text></text></number>	vip enable	Makes connections using the VIP name.
clrscrn  Clears the screen.  default protocol  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.  Change to config host level  name <text>  Sets the name of the host. <text> = name of the host.  Clears the name of the host.  To remote address  Clears the remote address of the host.  Clears the SSH username associated with the host.  protocol ssh  Sets the protocol to Telnet.</text></text>	vip name <text></text>	Sets the VIP name.
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>       Change to config host level         name <text>       Sets the name of the host.         <text> = name of the 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.</text></text></number>	write	Stores the current configuration in permanent memory.
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>       Change to config host level         name <text>       Sets the name of the host.         <text> = name of the 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.         Sets the protocol to Telnet.</text></text></number>	host 15 (config-host:15) level commands	
default remote port  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> Sets the name of the host.  Clears the name of the host.  Clears the remote address of the host.  Clears the remote address of the host.  Clears the SSH username associated with the host.  protocol ssh Sets the protocol to SSH.  Sets the protocol to Telnet.</text>	clrscrn	Clears the screen.
default value, which depends on the selected protocol.  Exits to the configuration level.  host <number> Change to config host level  name <text> 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 remote address of the host.  Clears the SSH username associated with the host.  protocol ssh Sets the protocol to SSH.  Sets the protocol to Telnet.</text></text></number>	default protocol	Restores the default value of the protocol (Telnet).
host <number> 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 remote address of the host.  Clears the SSH username associated with the host.  protocol ssh Sets the protocol to SSH.  Sets the protocol to Telnet.</text></number>	default remote port	default value,
name <text>  Sets the name of the host. <text> = name of the host.  no name  Clears the name of the host.  Clears the remote address of the host.  Clears the remote address of the host.  Clears the remote address of the host.  Clears the SSH username associated with the host.  protocol ssh  Sets the protocol to SSH.  Sets the protocol to Telnet.</text></text>	exit	Exits to the configuration level.
<text>= name of the 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.</text>	host <number></number>	Change to config host level
no remote address  Clears the remote address of the host.  Clears the SSH username associated with the host.  protocol ssh  Sets the protocol to SSH.  protocol telnet  Sets the protocol to Telnet.	name <text></text>	
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.	no name	Clears the name of the host.
protocol ssh Sets the protocol to SSH. protocol telnet Sets the protocol to Telnet.	no remote address	Clears the remote address of the host.
protocol telnet Sets the protocol to Telnet.	no ssh username	Clears the SSH username associated with the host.
	protocol ssh	Sets the protocol to SSH.
remote address <text> Sets the IP address of the remote host to connect to when</text>	protocol telnet	Sets the protocol to Telnet.
	remote address <text></text>	Sets the IP address of the remote host to connect to when

	T 1
	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) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:15:16) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices.

	<text> = SSH user name.</text>
to be an alive will accorde	
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:14:16) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:13:16) 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

Sets the connect tunnel AES encrypt key 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		T
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puncturation: 123ABC*123ABC*123ABC*123ABC*123ABC*123AbC*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.  auto show statistics clrscm  Clears the screen.  Clears the screen.  Credentials <fext>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connect to selection.  Removes the remote port used to establish tunnel connect to port used to establish tunnel connect port of used to establish tunnel connect port to use for connect mode tunneling.  Protocol type and the port to use for c</fext>		Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics cirscrn Clears the screen. Clears the screen. Clears the screen.  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address Removes the remote host address used to establish tunneling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no credentials Clears the RSA/DSA certificate selection.  no port Removes the connect unnel AES encrypt key.  no credentials Clears the RSA/DSA certificate selection.  no port Removes the sSH user name.  no top keep alive Disables the connect mode TCP keep alive timeout.  no vip name Removes the SSH user name.  Sets the remote port to use for connect mode tunneling.  volumber> Sets the remote port to use for connect mode tunneling.  protocol ssh Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Protocol top Uses TCP protocol for connect mode tunneling.  protocol top uses TCP protocol with AES encryption for connect mode tunneling.  protocol dep protocol dep Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol dep protocol dep Uses UDP protocol for connect mode tunneling.  Protocol dep Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
cirsorn  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 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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.  Removes the remote port used to establish tunnel connections.  no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  runmber&gt;  sets the remote port to use for connect mode tunneling.  runmber&gt;  protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP protocol for connect mode tunneling.  protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tep aes  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show bistory  Displays the last 20 commands entered during the current CLI session.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <fext>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt 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 VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SSL protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol telnet  Uses UDP protocol (with IAC) for connect mode tunneling.  Protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp  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.</fext>	auto show statistics	show connection statistics
client.  default protocol  default top keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Ro aes decrypt key  Removes the connect tunnel AES decrypt key.  Ro credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Ro vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssl  Uses SSL protocol for connect mode tunneling.  protocol top  Uses TCP protocol for connect mode tunneling.  protocol top aes  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show the current configuration.  Show the current configuration.  Displays the last 20 commands entered during the current CLI session.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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 SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling.  Protocol udp Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use 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.  Protocol 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.	credentials <text></text>	
exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  no top keep alive Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp Uses UDP protocol (with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	default protocol	Restores the default protocol as "TCP".
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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> Sets the remote port to use for connect mode tunneling.  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.  Protocol tep aes  Uses Tenet protocol (with IAC) for connect mode tunneling.  Uses Tenet protocol (with IAC) for connect mode tunneling.  Protocol udp  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.	default tcp keep alive	· ·
neling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no aes encrypt key Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <a href="mailto:rnumber">rnumber</a> Sets the remote port to use for connect mode tunneling.  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 UDP protocol for connect mode tunneling.  protocol 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.	exit	Exits to the next higher level.
no aes 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.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh Uses SSH protocol for connect mode tunneling.  Protocol tcp Uses TCP protocol for connect mode tunneling.  Protocol telnet Uses TCP protocol (with IAC) for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp 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.  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  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 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.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Uses TCP 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.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.  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.  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.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  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.  Protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP 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.	no port	
no vip name  Removes the VIP name.  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses TCP protocol for connect mode tunneling.  Uses UDP protocol (with IAC) 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.	no ssh username	Removes the SSH user name.
port <number></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
cnumber> = number of the port to use.   protocol ssh	no vip name	Removes the VIP name.
protocol ssl  protocol tcp  protocol tcp  protocol tcp aes  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.  protocol udp  protocol udp  protocol udp aes  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.	port <number></number>	Sets the remote port to use for connect mode tunneling. <pre></pre> <pre><pre><pre><pre><pre><pre><pr< td=""></pr<></pre></pre></pre></pre></pre></pre>
protocol tcp protocol tcp aes 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.  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.	protocol ssh	Uses SSH 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.  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.	protocol ssl	Uses SSL protocol for connect mode tunneling.
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  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.	protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol udp  protocol udp aes  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.	protocol tcp aes	
protocol udp aes  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.	protocol telnet	i. ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '
tunneling.  show Shows the current configuration.  show history Displays the last 20 commands entered during the current CLI session.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the current CLI session.	protocol udp aes	
CLI session.	show	Shows the current configuration.
show statistics show connection statistics	show history	
	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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:12:16) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:11:16) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:10:16) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:9:16) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
aes decrypt key <hexadecimal></hexadecimal>	<pre><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.</text></pre>

	Bytes may run together or be separated by optional punctuation: 123ABC "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
aes encrypt key <hexadecimal></hexadecimal>	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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:7:16) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 mode
protocol tcp aes	tunneling.

protocol udp aes    Uses UDP protocol with AES encryption tunneling.	tunneling.
show history  Displays the last 20 commands entered CLI session.  show statistics  sh username <text>  Sets the SSH user name for use when eneling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mosets the timer. <milliseconds> = timer value, in milliseconds = timer</milliseconds></milliseconds></text></text>	ion for connect mode
show statistics show connection statistics ssh username <text> Sets the SSH user name for use when a neling connections with other devices. <a href="text-2">text-2</a> SSH user name for use when a neling connections with other devices. <a href="text-2">text-2</a> SSH user name. top keep alive <milliseconds>  It pables TCP keep alive for connect mosets the timer.  williseconds&gt; = timer value, in milliseconds = timer value, in m</milliseconds></text>	
ssh username <text>  Sets the SSH user name for use when eneling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mosets the timer. <milliseconds> = timer value, in milliseconds = timer value, in milliseco</milliseconds></milliseconds></text></text>	ed during the current
neling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mo sets the timer. <milliseconds> = timer value, in milliseconds sets the timer. <milliseconds> = timer value, in milliseconds sets the timer. <milliseconds> = timer value, in milliseconds sets the timer. <milliseconds> = timer value, in milliseconds sets the timer. <milliseconds> = timer value, in milliseconds sets the vimer value, in milliseconds sets the timer. <milliseconds> = timer value, in milliseconds sets the vimer value, in milliseconds sets the vimer value, in milliseconds sets the set value suit on the server certificate ing.  Validate certificate disable  Nakes connections using the vIP name.  Sets the VIP name.  Sets the VIP name.  Sets the vIP name.  Sets the current configuration in perm.  Sets the fourth configuration in perm.  Sets the current configuration in perm.  Sets the current configuration in perm.  Sets the current configuration in perm.  Sets the connect tunnel AES decrypt ke bytes.  Each byte is represented by two adjaces.  Sets the connect tunnel AES decrypt ke bytes.  Each byte is represented by a single chance that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjaces bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  aes encrypt key <hexadecimal>  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjaces Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjaces Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enc</hexadecimal></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></text>	
sets the timer. <pre>   validate certificate disable   Skips verification of the server certificate ing.   validate certificate enable   Requires verification of the server certificate ing.   validate certificate enable   Requires verification of the server certificate ing.   vip disable   Makes connections using the specified // wip enable   Makes connections using the VIP name     vip enable   With   Stores the VIP name   Stores the current configuration in permital to tunnel connect-host:6:16)   level commands     address &lt; text&gt;   Sets the remote host to establish tunnel with     ctxxt&gt; = IP address or host name of the     aes decrypt key &lt; hexadecimal&gt;   Sets the connect tunnel AES decrypt ke bytes     Each byte is represented by two adjacet Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bc Note that quotes must enclose the value spaces     aes decrypt key text &lt; text&gt;   Sets the connect tunnel AES decrypt ke bytes     Each byte is represented by a single chance in the connect tunnel AES encrypt ke bytes     Each byte is represented by two adjacet Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bC Note that quotes must enclose the value spaces     Sets the connect tunnel AES encrypt ke bytes     Each byte is represented by two adjacet Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12,3a,bC Note that quotes must enclose the value spaces     Sets the connect tunnel AES encrypt ke bytes     Sets the connect tunnel AES encrypt ke bytes</pre>	n establishing tun-
validate certificate enable  Requires verification of the server certifinecting.  Vip disable  Makes connections using the specified // Makes connections using the Server certifinecting.  With enable  Vip name < text>  Sets the VIP name.  Write  Stores the current configuration in permitost 16 (tunnel-connect-host:6:16) level commands  address < text>  Sets the remote host to establish tunnel with. <text> = IP address or host name of the bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  aes decrypt key <hexadecimal>  Sets the connect tunnel AES decrypt ke bytes.  Each byte is represented by a single chance Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Sets the connect tunnel AES encrypt ke</hexadecimal></text>	_
vip disable  vip enable  Makes connections using the specified / Makes connections using the VIP name vip name < text>  Sets the VIP name.  Stores the current configuration in permit state (tunnel-connect-host:6:16) level commands  address < text>  Sets the remote host to establish tunnel with. <a href="text">text</a> Sets the remote host to establish tunnel with. <a href="text">text</a> Sets the connect tunnel AES decrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  aes decrypt key text < text>  Sets the connect tunnel AES decrypt ke bytes.  Each byte is represented by a single chance that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes.  Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  aes encrypt key text < text>  Sets the connect tunnel AES encrypt ke spaces.	ate when connect-
vip enable       Makes connections using the VIP name         vip name <text>       Sets the VIP name.         write       Stores the current configuration in permitors 16 (tunnel-connect-host:6:16) level commands         address <text>       Sets the remote host to establish tunnel with.         dest the remote host to establish tunnel with.       Sets the connect tunnel AES decrypt ke bytes.         Each byte is represented by two adjacer Bytes may run together or be separated tuation:       123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.         aes decrypt key text <text>       Sets the connect tunnel AES decrypt ke bytes.         Each byte is represented by a single chance that quotes must enclose the value spaces.       Sets the connect tunnel AES encrypt ke bytes.         aes encrypt key <hexadecimal>       Sets the connect tunnel AES encrypt ke bytes.         Each byte is represented by two adjacer Bytes may run together or be separated tuation:       123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.         aes encrypt key text <text>       Sets the connect tunnel AES encrypt ke</text></hexadecimal></text></text></text>	rtificate when con-
vip name <text> Sets the VIP name.  Write Stores the current configuration in permitable that the current confi</text>	ed Address.
write    Stores the current configuration in perms	me.
address <text>  Sets the remote host to establish tunnel with. <text> = IP address or host name of the sets to establish tunnel with. <text> = IP address or host name of the sets the connect tunnel AES decrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  aes decrypt key text <text> Sets the connect tunnel AES decrypt ke bytes. Each byte is represented by a single chance that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke spaces.</text></text></text></text>	
aes decrypt key <hexadecimal>  Sets the remote host to establish tunnel with.  <text> = IP address or host name of the  Sets the connect tunnel AES decrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES decrypt ke bytes. Each byte is represented by a single chance that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by a single chance that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke spaces.  Sets the connect tunnel AES encrypt ke spaces.  Sets the connect tunnel AES encrypt ke spaces.</text></hexadecimal>	rmanent memory.
with. <text> = IP address or host name of the  aes decrypt key <hexadecimal>  Sets the connect tunnel AES decrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  aes decrypt key text <text> Sets the connect tunnel AES decrypt ke bytes. Each byte is represented by a single chance that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a,bc Note that quotes must enclose the value spaces.  sets the connect tunnel AES encrypt ke value spaces.  Sets the connect tunnel AES encrypt ke value spaces.</text></hexadecimal></text>	
bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  aes decrypt key text <text> Sets the connect tunnel AES decrypt ke bytes. Each byte is represented by a single chance Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacers Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke bytes. Each byte is represented by two adjacers Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  Sets the connect tunnel AES encrypt ke</text>	_
bytes. Each byte is represented by a single change of Note that quotes must enclose the value spaces.  aes encrypt key <hexadecimal>  Sets the connect tunnel AES encrypt key bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key text</text></hexadecimal>	acent hex digits. ted by optional punc-
bytes. Each byte is represented by two adjacer Bytes may run together or be separated tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc Note that quotes must enclose the value spaces.  aes encrypt key text <text> Sets the connect tunnel AES encrypt ke</text>	character.
	acent hex digits. ted by optional punc-
Each byte is represented by a single change of the value spaces.	character.
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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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
	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

with.    <ext> = IP address or host name of the remote host.   <ext> = 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 purctuation:   123ABC 12 3A BC 12 3A, BC 12.3a, bc 12.3a bc 1</ext></ext>	host 16 (tunnel-connect-host:3:16) 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 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 optional punctuation: 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 unnel AES encrypt key with up to 16 bytes.  Clears the screen.  Clears the screen.  Clears the default protocol as 'TCP'.  Restores the default protocol as 'TCP'.  Restores the default the second connect mode TCP keep alive timeout.  Exist to the next higher level.  Exist to the next higher level.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES decrypt key.  Removes the connect nunnel AES decrypt key.  Removes the connect nunnel AES decrypt key.  Removes the remote port used to establish tunnel connections.  Re	address <text></text>	_
bytes. Each byte is represented by two adjacent hex 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 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 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 encrypt key 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.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the encounter tunnel AES decrypt key.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Removes the connect munel AES encrypt key.  Removes the connect munel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the connect munel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the connect		<text> = IP address or host name of the remote host.</text>
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 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.  auto show statistics  clicars the screen.  Clears the screen.  Clears the screen.  Credentials <fext> Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  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 unnel 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 SSH user name.  No top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the SSH user name.  Removes the SPH user name.  Sets the remote port to use for connect mode tunneling.  Chumber&gt; enumber&gt; enumber enumber enumeling.</fext></hexadecimal>	aes decrypt key <i><hexadecimal></hexadecimal></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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 to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the termote port used to establish tunnel connections.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  **CHUMBERS** AUMBERS** PORTOR CONNECT TO SETABLE POR	aes decrypt key text < <i>text</i> >	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no port  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rounder> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	aes encrypt key <i><hexadecimal></hexadecimal></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel port  Removes the remote port used to establish tunnel port  Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  ort <number> Sets the remote port to use.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.</number>	aes encrypt key text < <i>text</i> >	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel on nections.  Removes the remote port used to establish tunnel connections.  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  protocol ssh  Uses SSL protocol for connect mode tunneling.	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roundber> = number of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rnumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Anumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  Protocol ssl  Uses SSL protocol for connect mode tunneling.	default protocol	Restores the default protocol as "TCP".
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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  cnumber> = number of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	default tcp keep alive	
neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	exit	Exits to the next higher level.
Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no address	
Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Removes the VIP name.  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.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  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.	no port	· ·
no vip name  Removes the VIP name.  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 ssh username	Removes the SSH user name.
port <number> 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></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
<pre>conumber = number of the port to use.</pre> protocol ssh Uses SSH protocol for connect mode tunneling. Uses SSL protocol for connect mode tunneling.	no vip name	Removes the VIP name.
protocol ssl Uses SSL protocol for connect mode tunneling.	port < <i>number</i> >	
	protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol tcp Uses TCP protocol for connect mode tunneling.	protocol ssl	Uses SSL protocol for connect mode tunneling.
	protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tep aes  Uses TCP protocol with AES encryption for connect mode tunneling, protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling, protocol udp  Uses UDP protocol for connect mode tunneling, uses UDP protocol with AES encryption for connect mode tunneling, show as the current configuration.  Shows the current configuration.  Shows the current configuration.  Shows 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.  staxt>— SSH user name.  top keep alive <mitiliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  «milliseconds&gt; = 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.  vip disable  Makes connections using the VIP name.  sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Tost 16 (tunnel-connect-host 2:16) level commands  address <text>  Sets the remote host to establish tunneling connections with.  **etw&gt; = 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.  ase encrypt key *chexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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 dig</text></mitiliseconds>		
ing. 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 statistics Show connection statistics Show connection statistics Show the SH user name for use when establishing tunneling connections with other devices name.  tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling and sets the timer.  **milliseconds&gt; = Enables TCP keep alive for connect mode tunneling and sets the timer.  **validate certificate disable Skips verification of the server certificate when connecting.  validate certificate enable Requires verification of the server certificate when connecting.  vip disable Makes connections using the specified Address.  vip name <text> Sets the VIP name.  Sets the current configuration in permanent memory.  **Tost19 (tunnel-connect-host-2-16) level commands*  address   **Sets the remote host to establish tunneling connections with.  **Text&gt; = 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 1</text></milliseconds>	protocol tcp aes	
protocol udp aes  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 name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  vip disable  Vip disable  Makes connections using the specified Address.  vip enable  Vip name <fext></fext>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 16 (tunnel-connect-host-2:16) level commands  address <fext></fext>  Sets the remote host to establish tunneling connections with.  sets yell 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 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 12.3</milliseconds></milliseconds>	protocol telnet	l.
show Shows the current configuration.  Show listory  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.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  - milliseconds&gt; = 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.  vip disable  Makes connections using the specified Address.  vip enable  Wakes connections using the VIP name.  vip arme <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Tost 16 (tunnel-connect-inost-2:16) level commands  address <text>  Sets the verification of the server certificate when connections with.  - text&gt; = 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.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by woo adjacent hex 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.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC*12.3A BC*12.3ABC*12.3ABC*12.3a.bc 12.3a.bc  Note that quotes must enclose the value if it contains spaces.  Sets the connect tunnel AES encrypt k</text></text></milliseconds>	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  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.  It pkeep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  It pkeep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  It pkeep alive entificate disable  Skips verification of the server certificate when connecting.  Validate certificate enable  Requires verification of the server certificate when connecting.  Vip disable  Makes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 16 (tunnel-connect-host:2:16) level commands  address   Sets the remote host to establish tunneling connections with.  In the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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 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 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:  123 ABC</milliseconds></milliseconds>	protocol udp aes	
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text></text>	show history	
neling connections with other devices.	show statistics	show connection statistics
sets the timer. <pre><milliseconds> = timer 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Nost 16 (tunnel-connect-host:2:16) level commands  address < text>  Sets the remote host to establish tunneling connections with.  <	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the Specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 16 (tunnel-connect-host:2:16) level commands  address   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.  aes decrypt key <a href="hexadecimal">hexadecimal</a>  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  vip enable  vip enable  vip name < text>  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  host 16 (tunnel-connect-host:2:16) level commands  address < text>  Sets the remote host to establish tunneling connections with. <a href="https://docs.org/remove-text-">dext-</a> Sets the remote host to establish tunneling connections with. <a href="https://docs.org/remove-text-">dext-</a> Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "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 two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "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.	validate certificate disable	l. ·
vip enable vip name <text> Sets the VIP name. Sets the VIP name. Stores the current configuration in permanent memory.  host 16 (tunnel-connect-host:2:16) 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 optional punctuation: 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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 16 (tunnel-connect-host:2:16) level commands  address <text> Sets the remote host to establish tunneling connections with.    ext = 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.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunn</text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.	vip enable	Makes connections using the VIP name.
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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vin name <text></text>	Sets the VIP name
aes decrypt key <hexadecimal>  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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></hexadecimal>	IND HALLO STORES	Coto tilo vii lialilo.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text>	·	
aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></hexadecimal>	write	
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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.</text></hexadecimal>	write host 16 (tunnel-connect-host:2:16) level commands	Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	write 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.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	write host 16 (tunnel-connect-host:2:16) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	write host 16 (tunnel-connect-host:2:16) level commands address <text> aes decrypt key <hexadecimal> aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:1:16) level commands	S
address <text></text>	Sets the remote host to establish tunneling connections with.
	<pre><text> = IP address or host name of the remote host.</text></pre>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
	Chamber > = hamber of the port to use.

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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (config-host:16) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
	restores are detaunt rands or and protester ( 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 exit	Sets the remote port (used to connect to the host) to the default value,
	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 <number></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.
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.  Sets the protocol to Telnet.</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 menu.</text>

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. <a href="text"><a href="text"></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>

	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 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>	
·	CLI session.  Sets the username for logging into the host via SSH.
ssh username <text></text>	CLI session.  Sets the username for logging into the host via SSH. <text> = username.</text>
ssh username <text> write</text>	CLI session.  Sets the username for logging into the host via SSH. <text> = username.</text>
ssh username <text> write host 2 (tunnel-connect-host:16:2) level commands</text>	CLI session.  Sets the username for logging into the host via SSH. <text> = username.  Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.</text>

	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun-

	T
	neling connections with other devices.
	<pre>vitn other devices.</pre> <pre><text> = SSH user name.</text></pre>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and
top keep alive	sets the timer.
	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
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></text>	Sets the connect tunnel AES decrypt key with up to 16
aco decrypt key text stoxis	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:14:2) 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>	Sets the connect tunnel AES encrypt key 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:13:2) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.

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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:12:2) 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 <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,		
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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</hexadecimal>		· ·
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puncturation: 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. Ciercm contains spaces. Sets the connect unnel AES encrypt key 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 cliert. Ciercm contains spaces. Ciercm credentials  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client. default protocol Restores the default protocol as "TCP". default protocol Restores the default protocol as "TCP". Exist to the next higher level. Removes the default 45 second connect mode TCP keep alive timeout. Exist to the next higher level. Removes the remote host address used to establish tunneling connections. Removes the connect unnel AES decrypt key. Removes the connect unnel AES decrypt key. Removes the connect unnel 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 VIP name. Disables the connect mode TCP keep alive timeout. Removes the VIP name. Sets the remote port to use for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol ssh Uses SSH protocol for connect mode tunneling. Protocol top Uses TCP protocol for connect mode tunneling. Protocol top Uses TCP protocol (with IAC) for connect mode tunneling. Protocol udp Uses UDP protocol (with AES encryption for connect mode tunneling.	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics  cirscrn  Clears the screen.  credentials < text>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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 encrypt key.  credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no port  Removes the semole port used to establish tunnel connections.  no port  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rumber>  sets the remote port to use for connect mode tunneling.  rumber>  protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol for connect mode tunneling.  protocol tcp  uses TCP protocol (with AES encryption for connect mode tunneling.  protocol tcp  Uses TCP protocol (with AES encryption for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
cirscm  Clears the screen.  Credentials <a href="text">text</a> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh Uses SSH protocol for connect mode tunneling.  protocol ssl Uses SSL protocol for connect mode tunneling.  protocol tcp Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tcp aes Uses USP protocol (with IAC) for connect mode tunneling.  protocol udp Uses USP protocol with AES encryption for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses USP protocol with AES encryption for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.  Protocol udp Protocol with AES encryption for connect mode tunneling.  Uses USP Protocol with AES encryption for connect mode tunneling.  Uses USP Protocol with AES encryption for connect mode tunneling.	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol  default top keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the remote port used to establish tunnel connections.  no stop keep alive  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssl  Uses SSL protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tcp aes  Uses USP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses USP protocol with AES encryption for connect mode tunneling.  Uses USP protocol with AES encryption for connect mode tunneling.</text>	auto show statistics	show connection statistics
client.  default protocol  default top keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssl  Uses SSL protocol for connect mode tunneling.  protocol tcp  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tep aes  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.  Uses UDP protocol with AES encryption for connect mode tunneling.	clrscrn	Clears the screen.
default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the VIP name.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Anumber>  protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol top  Uses TCP protocol for connect mode tunneling.  protocol tep aes  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  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.	credentials <text></text>	· ·
alive timeout.  Exits to the next higher level.  no address  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 connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	default protocol	Restores the default protocol as "TCP".
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 connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 udp  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.  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.</number>	default tcp keep alive	· ·
neling connections.  no aes decrypt key  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber>  Sets the remote port to use for connect mode tunneling.  Lyses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  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.  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the VIP name.  Port <a href="mailto:number">no top keep alive timeout.</a> Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  **enumber*> = number of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol top  Uses TCP protocol for connect mode tunneling.  protocol top aes  Uses TCP protocol (with AES encryption for connect mode tunneling.)  protocol telnet  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.  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.  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the VIP name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> sets the remote port to use.  Disables the connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Disables the connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Disables the 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.  Disables the remote port used tunneling.  Uses TCP protocol for connect mode tunneling.  Uses TCP protocol with AES encryption for connect mode tunneling.  Disables the remote port used tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber>  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 udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  Sets the remote port to use for connect mode tunneling.  I uses SSH protocol for connect mode tunneling.  Protocol ssl  Uses SSL protocol for connect mode tunneling.  Uses TCP 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.  Protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.</number>	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  number> = number of the port to use.  protocol ssh  Disables the connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Number> = number of the port to use.  Disables the connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Disables the connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP protocol for connect mode tunneling.  Disables the connect mode tunneling.  Uses TCP protocol for connect mode tunneling.  Uses TCP protocol (with IAC) for connect mode tunneling.  Disables the connect mode tunneling.  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	no port	
no vip name  port <number>  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  Uses SSL protocol for connect mode tunneling.  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.  protocol udp  protocol udp  protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.</number></number>	no ssh username	Removes the SSH user name.
port <number> 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 tcp aes Uses TCP protocol (with IAC) for connect mode tunneling.  protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.</number></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
cnumber> = number of the port to use.   protocol ssh	no vip name	
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.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	port <number></number>	
protocol tcp  protocol tcp aes  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	protocol ssh	
protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	protocol ssl	Uses SSL protocol for connect mode tunneling.
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	protocol tcp	
protocol udp Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.	protocol tcp aes	tunneling.
protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.	protocol telnet	I.
tunneling.	protocol udp	Uses UDP protocol for connect mode tunneling.
show Shows the current configuration.	protocol udp aes	
	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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep
default tcp keep alive	Restores the default 45 second connect mode TCP keep

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:10:2) 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></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
aes encrypt key <hexadecimal></hexadecimal>	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 guotes must enclose the value if it contains
aes encrypt key text <text></text>	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
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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:9:2) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:8:2) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 mode
protocol tcp aes	tunneling.

	l., ., , , , , , , , , , , , , , , , ,
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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>	Sets the connect tunnel AES encrypt key 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:6:2) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:5:2) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

host 2 (tunnel-connect-host:4:2) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 top aes  Uses TCP protocol with AES encryption for connect mode tunneling, protocol telnet  Uses TIP protocol (with IAC) for connect mode tunneling, 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 Ishow  Show ishe current configuration.  Displays the last 20 commands entered during 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.  top keep alive <milliseconds>  statistics = 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.  Validate certificate enable  Requires 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.  Validate certificate enable  Requires 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.  Validate certificate enable  Requires 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.  Validate certificate enable  Requires verification of the server certificate when connecting.  Sets the VIP name.  Vip name    Validate Certificate enable  Sets the VIP name.  Validate Certificate when connecting.  Sets the connect tunnel AES decrypt key with</milliseconds>		
Ing.   Uses UDP protocol for connect mode tunneling.	protocol tcp aes	
Uses UDP protocol with AES encryption for connect mode tunneling.	protocol telnet	l.
tunneling.	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.  - devi = SSH user name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  - milliseconds&gt; as the timer.  - milliseconds in timer value, in milliseconds.  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 2 (tunnel-connect-host:3:2) level commands  address <text>  Sets the remote host to establish tunneling connections with.  - devi = 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.  aes encrypt key <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 <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:  123.ABC 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 encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run toge</hexadecimal></hexadecimal></text></text></milliseconds>	protocol udp aes	
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices.   tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip name <text> Sets the VIP name.   write Stores the current configuration in permanent memory.   host2 (tunnel-connect-host3x2) level commands   address <text> Sets the remote host to establish tunneling connections with.   <text>= IP address or host name of the remote host.   aes decrypt key <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   123ABC *12 3A BC* 12.3a bc 12.3a bc vote that quotes must enclose the value if it contains spaces.   aes encrypt key <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</hexadecimal></hexadecimal></text></text></text></milliseconds></milliseconds>	show history	
neling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling 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.  Wakes connections using the specified Address.  Wakes connections using the specified Address.  Wakes connections using the VIP name.  Vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 2 (tunnel-connect-host:3:2) 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.  Beach byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12,3a,bc 12:3a:bc  Note that quotes must enclose the value if it contains spaces.  Best he connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains spaces.  Best byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains spaces.  Best the connect tunnel AES encrypt key with up to 16 bytes.  Best he connect tunnel AES encrypt key with up to 16 bytes.  Best byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains spaces.  Best the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text></milliseconds></text>	show statistics	show connection statistics
sets the timer. <pre></pre>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 2 (tunnel-connect-host:3:2) 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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  host 2 (tunnel-connect-host:3:2) 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 optional punctuation:  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 two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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.</text></text>	validate certificate disable	l. '
vip enable  vip name <text> Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 2 (tunnel-connect-host:3:2) 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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 2 (tunnel-connect-host:3:2) 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 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 encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Stores the current cu	vip enable	Makes connections using the VIP name.
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 optional punctuation: 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vip name <text></text>	Sets the VIP name.
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 optional punctuation: 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>		
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text>	write	Stores the current configuration in permanent memory.
aes decrypt key <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.  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</hexadecimal>	- 12	Stores the current configuration in permanent memory.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	host 2 (tunnel-connect-host:3:2) level commands	Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES encrypt key with up to 16 bytes.	host 2 (tunnel-connect-host:3:2) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	host 2 (tunnel-connect-host:3:2) level commands address <text>  aes decrypt key <hexadecimal></hexadecimal></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</text>
	host 2 (tunnel-connect-host:3:2) level commands address <text>  aes decrypt key <hexadecimal>  aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:2:2) level commands	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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
	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.
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>  tcp keep alive <milliseconds></milliseconds></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and</text>
top keep alive	sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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
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 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. <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 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></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 22 (config-host:22) 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	
<u>'</u>	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 23 (config-host:23) 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. <a href="text"><text> = username.</text></a>
write	Stores the current configuration in permanent memory.
host 24 (config-host:24) 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.

Change to config host level
Sets the name of the host.
<text> = name of the host.</text>
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.</text>
Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
Sets the username for logging into the host via SSH. <text> = username.</text>
Stores the current configuration in permanent memory.
Clears the screen.
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.
Exits to the configuration level.
Change to config host level
Sets the name of the host. <text> = name of the host.</text>
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.</text>
1
Sets the remote port used to connect to the host. <pre><number> = port to be used.</number></pre>
· ·
<pre><number> = port to be used. Displays the current configuration.</number></pre>
<pre><number> = port to be used. Displays the current configuration. Displays the last 20 commands entered during the current</number></pre>
<pre><number> = port to be used. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the username for logging into the host via SSH.</number></pre>
<pre><number> = port to be used. Displays the current configuration. Displays the last 20 commands entered during the current CLI session. Sets the username for logging into the host via SSH. <text> = username.</text></number></pre>

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,
exit	which depends on the selected protocol.  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>
ita	Change the assument configuration is a supercontinuous
write	Stores the current configuration in permanent memory.
host 27 (config-host:27) level commands	Stores the current configuration in permanent memory.
	Clears the screen.
host 27 (config-host:27) level commands	
host 27 (config-host:27) level commands clrscrn	Clears the screen.
host 27 (config-host:27) level commands clrscrn default protocol	Clears the screen.  Restores the default value of the protocol (Telnet).  Sets the remote port (used to connect to the host) to the default value,
host 27 (config-host:27) level commands cirscrn default protocol default remote port	Clears the screen.  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.
host 27 (config-host:27) level commands clrscrn default protocol default remote port exit	Clears the screen.  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.  Exits to the configuration level.
host 27 (config-host:27) level commands clrscrn default protocol default remote port  exit host <number></number>	Clears the screen.  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.  Exits to the configuration level.  Change to config host level  Sets the name of the host.
host 27 (config-host:27) level commands clrscrn default protocol default remote port  exit host <number> name <text></text></number>	Clears the screen.  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.  Exits to the configuration level.  Change to config host level  Sets the name of the host. <text> = name of the host.</text>
host 27 (config-host:27) level commands  clrscrn  default protocol  default remote port  exit  host <number> name <text>  no name</text></number>	Clears the screen.  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.  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>
host 27 (config-host:27) level commands  clrscrn  default protocol  default remote port  exit  host <number> no name no remote address</number>	Clears the screen.  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.  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>
host 27 (config-host:27) level commands  clrscrn  default protocol  default remote port  exit  host <number> name <text>  no name  no remote address no ssh username</text></number>	Clears the screen.  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.  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>
host 27 (config-host:27) level commands  clrscrn  default protocol  default remote port  exit  host <number> no name  no remote address no ssh username  protocol ssh</number>	Clears the screen.  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.  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>
host 27 (config-host:27) level commands  clrscrn  default protocol  default remote port  exit  host <number> name <text>  no name no remote address no ssh username protocol ssh protocol telnet</text></number>	Clears the screen.  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.  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 menu.</text>
host 27 (config-host:27) level commands  clrscrn  default protocol  default remote port  exit  host <number> name <text>  no name no remote address no ssh username protocol ssh protocol telnet  remote address <text></text></text></number>	Clears the screen.  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.  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 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>

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

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. <a href="text"><text> = username.</text></a>
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:16:3) 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
add decrypt toy should commany	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.

no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:15:3) 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 < <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
, , , , , , , , , , , , , , , , , , ,	71 7 1 7 1

aes encrypt key text < text>  auto show statistics clrscrn	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and

Skips verification of the server certificate when connecting.		sets the timer.
ing.  Requires verification of the server certificate when connections, vip disable  Makes connections using the specified Address. vip enable  Makes connections using the VIP name.  Sets the virture configuration in permanent memory.  Nost 3 (funnel-connect-host:14:3) level commands address < rext>  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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 decrypt key 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 because 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	validata contificata disphi-	<milliseconds> = timer value, in milliseconds. China varification of the convex contificate when connect</milliseconds>
necting.  Makes connections using the specified Address.  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Makes connect the connect thost: 14:3) level commands  address < fext>  Sets the remote host to establish tunneling connections with.		ing.
Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Some view visit	validate certificate enable	
Sets the VIP name   Sets the current configuration in permanent memory.	vip disable	Makes connections using the specified Address.
Stores the current configuration in permanent memory.  **nost 3 (tunnel-connect-host:14:3) level commands**  **address < text>***  Sets the remote host to establish tunneling connections with.  **ale decrypt key < thexadecimal>**  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex 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 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	vip enable	Makes connections using the VIP name.
Sets the remote host to establish tunneling connections with.    Sets the connect tunnel AES decrypt key with up to 16 bytes.	vip name <text></text>	Sets the VIP name.
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.  Back byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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 12,3a,bc hyte is represented by two adjacent hex 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 encrypt key 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.  Sets the screen.  Set she screen.	write	Stores the current configuration in permanent memory.
with.	host 3 (tunnel-connect-host:14:3) level comma	ands
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 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. 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.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the remote host address used to establish tunneling connections.	address <text></text>	with.
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.  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".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  Bets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Bets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Bets 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".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES decrypt key.	aes decrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics  clirscrn  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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>	aes encrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  default tcp keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	default protocol	Restores the default protocol as "TCP".
Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	default tcp keep alive	·
neling connections.  no aes decrypt key  no aes encrypt key  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	exit	Exits to the next higher level.
no aes encrypt key Removes the connect tunnel AES encrypt key.	no address	
	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no credentials Clears the RSA/DSA certificate selection.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
	no credentials	Clears the RSA/DSA certificate selection.

no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:13:3) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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>	Sets the connect tunnel AES encrypt key 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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.

no ses encrynt key	Pamoves the connect tunnel AES energet key
no aes encrypt key no credentials	Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:11:3) 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
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

	<u> </u>
	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:10:3) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:9:3) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:8:3) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep
default tcp keep alive	Restores the default 45 second connect mode TCP keep

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:7:3) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 top keep alive	Restores the default 45 second connect mode TCP keep
default top keep alive	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:5:3) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 mode
protocol tcp aes	tunneling.

show Shows the current configuration.  Show history Displays the last 20 commands entered during the current CLI session.  Show statistics Show connection statistics Show connection statistics Show connections show the current configuration and sets the state of the connections with other devices.  Leave = SSH user name for use when establishing tunneling connections with other devices.  Leave = SSH user name.  Enables TCP keep alive for connect mode tunneling and sets the timer.  Amilliseconds> = timer value, in milliseconds.  Skips verification of the server certificate when connecting.  Validate certificate enable Requires verification of the server certificate when connecting.  Vip disable Makes connections using the specified Address.  Vip enable Makes connections using the VIP name.  Vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 3 (tunnel-connect-host:4:3) level commands  address <text> Sets the remote host to establish tunneling connections with.  Letx'= 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.  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.  Sets the connect tunnel AES decrypt key 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.  Each byte is represented by two adjacent hex digits.  Each byte is represented by two adjacent hex digits.</text></text></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  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.  **clexb** = SSH user name.**  top keep alive **cmilliseconds**>  Enables TCP keep alive for connect mode tunneling and sets the timer.  **cmilliseconds** = 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.  vip disable  Makes connections using the specified Address.  vip enable  vip name <fext>  Sets the VIP name.  vip name <fext>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost3 (tunnel-connect-hosts43) level commands  address <fext>  Sets the remote host to establish tunneling connections with.  **access of the server service the value if it contains spaces.  Best decrypt key <fexadecimal>  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC 12 3A BC 12 3A BC 12.3a bc 12:3a-bc  Note that quotes must enclose the value if it contains spaces.  Best monnect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC 12 3A BC 12.3a BC 12.3a bc 12:3a-bc  Note that quotes must enclose the value if it contains spaces.  Best monnect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Best byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Best byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  But show connection sta</fexadecimal></fext></fext></fext>	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
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.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  -milliseconds&gt; = 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Rost3 (tunnel-connect-host43) level commands  address <text>  Sets the remote host to establish tunneling connections with.  -text&gt; = IP address or host name of the remote host.  aes decrypt key <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 encrypt key <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 <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 16 bytes.  Each byte is represented by a single character.  Note</hexadecimal></hexadecimal></hexadecimal></text></text></milliseconds>	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices.	show history	Displays the last 20 commands entered during the current CLI session.
neling connections with other devices   <text> = SSH user name.    </text>	show statistics	show connection statistics
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.  vip disable  Makes connections using the specified Address.  vip enable  vip name <text>  Sets the VIP name.  vip name <text>  Sets the VIP name.  vip name <text>  Sets the current configuration in permanent memory.  **nost3 (tunnel-connect-host4:3) level commands*  address <text>  Sets the remote host to establish tunneling connections with.  **stext= IP address or host name of the remote host.  aes decrypt key <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 encrypt key <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 *</hexadecimal></hexadecimal></text></text></text></text>	ssh username <text></text>	neling connections with other devices.
ing.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  vip name <text>  Sets the VIP name.  write  Stores the current configuration in permanent memory.  Nost 3 (tunnel-connect-host:4:3) level commands  address &lt; text&gt;  Sets the remote host to establish tunneling connections with.  <te>  aes decrypt key &lt; hexadecimal&gt;   Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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</te></text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
vip disable vip disable vip enable vip enable vip name <text> Sets the VIP name.  Write Stores the current configuration in permanent memory.  Nost 3 (tunnel-connect-host:4:3) 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: 1233ABC *12.3A.BC 12.3a.bc 12.3a.bc Note that quotes must enclose the value if it contains spaces.  aes encrypt key <hexadecimal> Sets the connect tunnel AES decrypt key 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</hexadecimal></text></text></text>	validate certificate disable	
vip enable       Makes connections using the VIP name.         vip name <text>       Sets the VIP name.         write       Stores the current configuration in permanent memory.         host 3 (unnel-connect-host:4:3) level commands         address <text>       Sets the remote host to establish tunneling connections with.         .text&gt; = 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.         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>       Sets the connect tunnel AES encrypt key with up to 16 bytes.         Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:         123ABC "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.&lt;</text></hexadecimal></text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 3 (tunnel-connect-host:4:3) 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 optional punctuation: 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.</text></text></text>	vip disable	Makes connections using the specified Address.
write    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.     Actext> = 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 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.	vip enable	Makes connections using the VIP name.
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 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.  auto show statistics</text></text>	vip name <text></text>	Sets the VIP name.
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 optional punctuation:  123ABC "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 two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.</text></text></text>	write	Stores the current configuration in permanent memory.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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</text></text>	host 3 (tunnel-connect-host:4:3) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics	address <text></text>	with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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</text></hexadecimal>		1
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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</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
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		Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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
	aes decrypt key text < 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
clrscrn Clears the screen.	aes decrypt key text <text> aes encrypt key <hexadecimal></hexadecimal></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
<u> </u>	aes decrypt key text <text>  aes encrypt key <hexadecimal>  aes encrypt key text <text></text></hexadecimal></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.

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:3:3) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

with.    staxt = IP address or host name of the remote host.	host 3 (tunnel-connect-host:1:3) level commands	
Sets the connect tunnel AES decrypt key with up to 16 bykes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A,BC 12.3a	address <text></text>	_
bytes. Each byte is represented by two adjacent hex 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 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		<text> = IP address or host name of the remote host.</text>
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.  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.  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exit to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the SSH user name.  Sets the remote port to use for connect mode tunneling.  contocol ssh  Uses SSH protocol for connect mode tunneling.	aes decrypt key <i><hexadecimal></hexadecimal></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Beach byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel on aes encrypt key Removes the remote port used to establish tunnel on sh username 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 to establish tunnel connections.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Control colors.  Uses SSH protocol for connect mode tunneling.	aes decrypt key text < <i>text</i> >	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 sSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  contocol ssh  Uses SSH protocol for connect mode tunneling.	aes encrypt key <i><hexadecimal></hexadecimal></i>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel or port Removes the remote port used to establish tunnel or nections.  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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <a href="https://www.no.con.org/no.con.org/">www.no.con.org/no.con.org/</a> Sets the remote port to use for connect mode tunneling.  Fortocol ssh Uses SSH protocol for connect mode tunneling.	aes encrypt key text < <i>text</i> >	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  control of the port to use.  Disables the port connect mode tunneling.  Clears the RSA/DSA certificate selection.  Removes the SSH protocol for connect mode tunneling.  Connections to use for connect mode tunneling.  Control of the port to use.  Disables the port connect mode tunneling.  Control of the port to use.  Control of the port to use.  Control of the port to use.  Control of connect mode tunneling.	auto show statistics	show connection statistics
client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 port used to establish tunnel no port  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 VIP name.  Sets the remote port to use for connect mode tunneling.  Annumber>  Protocol ssh  Uses SSH protocol for connect mode tunneling.	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rounder> enotocol ssh  Uses SSH protocol for connect mode tunneling.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  cont < number> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	default protocol	Restores the default protocol as "TCP".
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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  contended tunneling.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Sets user name.  Disables the connect mode TCP keep alive timeout.  Contended tunneling.  Contended tunneling.  Contended tunneling.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connect mode tunneling.  Contended tunneling.	default tcp keep alive	
neling 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	exit	Exits to the next higher level.
Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  cont < number> = number of the port to use.  Disables the connect mode tunneling.  Sets the remote port to use.  Uses SSH protocol for connect mode tunneling.	no address	
Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no top name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no credentials	Clears the RSA/DSA certificate selection.
Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  Sets the remote port to use for connect mode tunneling.  no vip name  Sets the remote port to use for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no port	· ·
Removes the VIP name.  Sets the remote port to use for connect mode tunneling. <pre>cont <number></number></pre> <pre>protocol ssh</pre> Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no ssh username	Removes the SSH user name.
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 tcp keep alive	Disables the connect mode TCP keep alive timeout.
<pre>converse</pre>	no vip name	Removes the VIP name.
protocol ssl Uses SSL protocol for connect mode tunneling.	port < <i>number</i> >	
	protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol tcp Uses TCP 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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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>
ahaur	Displays the current configuration.
show	Displays the current configuration.

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	<u> </u>
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 31 (config-host:31) 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 32 (config-host:32) 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 4 (tunnel-connect-host:16:4) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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>

no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:14:4) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun-

	neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:13:4) 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>	Sets the connect tunnel AES decrypt key 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:12:4) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun-
	neling connections
	with other devices. <text> = SSH user name.</text>
ton keen alive millioneende	
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.
	<pre><milliseconds> = timer value, in milliseconds.</milliseconds></pre>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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
aes decrypt key	bytes.
	Each byte is represented by two adjacent hex digits.
	Bytes may run together or be separated by optional punctuation:
	123ABC "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 punc-
	tuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.

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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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>	Sets the connect tunnel AES decrypt key 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:9:4) 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".

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:8:4) 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 <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
aes encrypt key <hexadecimal></hexadecimal>	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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:7:4) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep
default top keep alive	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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
ass assign noy should something	bytes.
	Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-
	tuation:
	123ABC "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
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16
aco chorypt key text stext?	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.

show S show history D show statistics ssh username < text> S tcp keep alive < milliseconds> E seconds	Uses UDP protocol with AES encryption for connect mode runneling.  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.  Atext> = SSH user name.  Enables TCP keep alive for connect mode tunneling and sets the timer.  Amilliseconds> = timer value, in milliseconds.
show history  Show statistics  show statistics  ssh username <text>  State of the s</text>	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.  stext> = SSH user name.  Enables TCP keep alive for connect mode tunneling and sets the timer.
show statistics ssh username <text>  ssh username <text>  ssh username <text>  tcp keep alive <milliseconds>  ssh username <text>  ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh username <text> ssh us</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></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></milliseconds></text></text></text>	CLI session.  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and sets the timer.</text>
ssh username <text>  S  n  w   tcp keep alive <milliseconds>    E  validate certificate disable</milliseconds></text>	Sets the SSH user name for use when establishing tun- neling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and sets the timer.</text>
tcp keep alive <milliseconds>  E so validate certificate disable</milliseconds>	neling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and sets the timer.</text>
validate certificate disable S	sets the timer.
Į ir	Skips verification of the server certificate when connect- ng.
	Requires verification of the server certificate when con- necting.
vip disable N	Makes connections using the specified Address.
vip enable M	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:5:4) level commands	
w	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
b E B tu 1.	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
b E	Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.
b E B tu 1.	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
b E	Sets the connect tunnel AES encrypt key 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 sl	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:4:4) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:3:4) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

host 4 (tunnel-connect-host:2:4) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 tep aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol teinet  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Show show the current configuration.  Show the current configuration.  Show show thistory  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.  Sets the SSH user name for use when establishing tunneling connections with other devices.  stext = SSH user name.  tcp keep alive **rmilliseconds**  Enables TCP keep alive for connect mode tunneling 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip oname <text>  write  Stores the vIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Institute = IP address or host name of the remote host.  Sets the vip 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*  Note that quotes must enclose the value if it contains spaces.  aes encrypt key &lt;*hexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC*12</text>		
ing.  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.  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 name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  «milliseconds» = timer value, in milliseconds.  Validate certificate disable  Skips verification of the server certificate when connecting.  Vip disable  Wakes connections using the specified Address.  Vip enable  Vip name <text> Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the vIP name and the remote host to establish tunneling connections with,   **etxt&gt; = IP address or host name of the remote host.  Sets the remote host to establish tunneling connections with,   **etxt&gt; = 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 *12,3ABC *12,3a,bc \$12,3a,bc \$1</text></milliseconds>	protocol tcp aes	
protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunnelling.  show  Shows the current configuration.  Displays the last 20 commands entered during the current CLI session.  show statistics  show connection statistics  show connections with other devices.  Sets the SSH user name for use when establishing tunneling connections with other devices name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  vip disable  vip disable  vip name <fext></fext> write  Stores the connections using the specified Address.  vip enable  Vip name <fext></fext> Sets the VIP name.  Stores the current configuration in permanent memory.  Sets the VIP name.  Stores the current configuration in permanent memory.  Notal (tunnel-connecti-host:1:4) level commands  address <fext></fext>  Sets the remote host to establish tunneling connections with.   <a 12="" 12,3a,bc="" 12.3a,bc="" 12:3a;bc="" 3a="" <hexadecimal="" aes="" bc"="" contains="" decrypt="" enclose="" href="https://www.new.new.new.new.new.new.new.new.new.&lt;/td&gt;&lt;td&gt;protocol telnet&lt;/td&gt;&lt;td&gt;I.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;show Shows the current configuration.  Show thistory 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. &lt;/td&gt;&lt;td&gt;protocol udp&lt;/td&gt;&lt;td&gt;Uses UDP protocol for connect mode tunneling.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;show history  Displays the last 20 commands entered during the current CLI session.  Show connection statistics  show statistics  Sets the SSH user name for use when establishing tunneling connections with other devices. &lt;/td&gt;&lt;td&gt;protocol udp aes&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;  CLI session.    &lt;/td&gt;&lt;td&gt;show&lt;/td&gt;&lt;td&gt;Shows the current configuration.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Sets the SSH user name for use when establishing tunneling connections with other devices.  top keep alive &lt;milliseconds&gt;  top keep alive &lt;milliseconds&gt;  Enables TCP keep alive for connect mode tunneling and sets the timer.  &lt;milliseconds&gt; = timer value, in milliseconds.  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the specified Address.  vip name &lt;text&gt; Sets the VIP name.  vithe Stores the current configuration in permanent memory.  host 4 (tunnel-connect-host:1:4) level commands  address &lt;text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = 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.  aes encrypt key &lt;hexadecimal&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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 12.3a.bc  Note that quotes must enclose the value if it contains spaces.  aes encrypt key text &lt;text&gt; Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.&lt;/td&gt;&lt;td&gt;show history&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;neling connections with other devices.   tcp keep alive &lt;milliliseconds&gt; Enables TCP keep alive for connect mode tunneling and sets the timer.  &lt;milliliseconds&gt; = 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip name &lt;text&gt; Sets the VIP name.   write Stores the current configuration in permanent memory.   nost 4 (tunnel-connect-host:1:4) level commands   address &lt;text&gt; Sets the remote host to establish tunneling connections with.   &lt;text&gt; = IP address or host name of the remote host.   aes decrypt key &lt;hexadecimal&gt; Sets the connect tunnel AES decrypt key with up to 16 bytes.   aes hyte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.   aes encrypt key &lt;hexadecimal&gt; Sets the connect tunnel AES encrypt key with up to 16 bytes.   aes hyte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a.bc   note that quotes must enclose the value if it contains spaces. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC *12 3A BC* 12,3A,BC 12.3a.bc 1&lt;/td&gt;&lt;td&gt;show statistics&lt;/td&gt;&lt;td&gt;show connection statistics&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;sets the timer.  &lt;milliseconds&gt; = 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  **Nost 4 (tunnel-connect-host:1:4) level commands**  address &lt; text&gt;  Sets the remote host to establish tunneling connections with.  &lt; &lt;/td&gt;&lt;td&gt;ssh username &lt;text&gt;&lt;/td&gt;&lt;td&gt;neling connections with other devices.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 4 (tunnel-connect-host:1:4) level commands  address &lt; text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = 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 " if="" it="" key="" must="" note="" quotes="" spaces.="" that="" the="" value="">  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</a></milliseconds>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name < text>  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the virrent configuration in permanent memory.  host 4 (tunnel-connect-host:1:4) level commands  address < text>  Sets the remote host to establish tunneling connections with.	validate certificate disable	I. ·
vip enable vip name <text> Sets the VIP name. Sets the VIP name. Stores the current configuration in permanent memory.  **Note 4 (tunnel-connect-host:1:4) level commands**  address <text>  **Sets the remote host to establish tunneling connections with.  **Atext&gt; = 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.  **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 &lt;*hexadecimal&gt;**  **Sets the connect tunnel AES encrypt key with up to 16 bytes.  **Each byte is represented by two adjacent hex digits.  **Bytes may run together or be separated by optional punctuation:  **123ABC "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 two adjacent hex digits.  **Bytes may run together or be separated by optional punctuation:  **123ABC "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.  **Sets the connect tunnel AES encrypt key with up to 16 bytes.  **Sets the connect tunnel AES encrypt key with up to 16 bytes.  **Sets the connect tunnel AES encrypt key with up to 16 bytes.  **Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text></text></text>	validate certificate enable	
vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 4 (tunnel-connect-host:1:4) level commands  address <text>  Sets the remote host to establish tunneling connections with.     Sets the connect tunnel AES decrypt key with up to 16 bytes.    </text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.	vip enable	Makes connections using the VIP name.
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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vip name <text></text>	Sets the VIP name
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.  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text></text>	List comme seems	octs the vir hame.
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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>		
aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></hexadecimal>	write	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text></text>	write host 4 (tunnel-connect-host:1:4) level commands	Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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.</text></hexadecimal>	write host 4 (tunnel-connect-host:1:4) level commands	Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	write host 4 (tunnel-connect-host:1:4) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	write host 4 (tunnel-connect-host:1:4) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	write host 4 (tunnel-connect-host:1:4) level commands address <text> aes decrypt key <hexadecimal> aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
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. <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 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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 con-
	necting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:15:5) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.

no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:14:5) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>

validate certificate disable	Skips verification of the server certificate when connect-
validate certificate enable	Requires verification of the server certificate when con-
	necting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.

no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:12:5) 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 <i><hexadecimal></hexadecimal></i>	Sets the connect tunnel AES encrypt key with up to 16
)	

aes encrypt key text < text>  auto show statistics clrscrn	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and

Skips verification of the server certificate when connecting.		sets the timer.
ing.  Requires verification of the server certificate when connections, vip disable  Makes connections using the specified Address. vip enable  Makes connections using the VIP name.  Sets the virture configuration in permanent memory.  Nost 5 (funnel-connect-host:11-5) level commands address < rext>  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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 decrypt key 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 because 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	validata contificata disable	<milliseconds> = timer value, in milliseconds. China varification of the convex contificate when connect</milliseconds>
necting.  Makes connections using the specified Address.  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Notest 5 (tunnel-connect-host:11:5) level commands  address <fext>  Sets the remote host to establish tunneling connections with. </fext>		ing.
Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Some view visit	validate certificate enable	
Sets the VIP name   Sets the current configuration in permanent memory.	vip disable	Makes connections using the specified Address.
Stores the current configuration in permanent memory.  **nost 5 (tunnel-connect-host:11:5) level commands**  **address < text>***  Sets the remote host to establish tunneling connections with.  **ale decrypt key < thexadecimal>**  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex 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 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	vip enable	Makes connections using the VIP name.
Sets the remote host to establish tunneling connections with.    Sets the connect tunnel AES decrypt key with up to 16 bytes.	vip name <text></text>	Sets the VIP name.
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.  Back byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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 12,3a,bc hyte is represented by two adjacent hex 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 encrypt key 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.  Sets the screen.  Set she screen.	write	Stores the current configuration in permanent memory.
with.	host 5 (tunnel-connect-host:11:5) level comma	ands
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 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. 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.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the remote host address used to establish tunneling connections.	address <text></text>	with.
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.  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".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  Best 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. Beauto show statistics  Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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>	aes decrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics  clirscrn  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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>	aes encrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  default tcp keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	default protocol	Restores the default protocol as "TCP".
Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	default tcp keep alive	·
neling connections.  no aes decrypt key  no aes encrypt key  Removes the connect tunnel AES decrypt key.  Removes the connect tunnel AES encrypt key.	exit	Exits to the next higher level.
no aes encrypt key Removes the connect tunnel AES encrypt key.	no address	
	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no credentials Clears the RSA/DSA certificate selection.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
·	no credentials	Clears the RSA/DSA certificate selection.

no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:10:5) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices.

	<text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:9:5) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.

	D 11 11 11 11 11 11 11 11 11 11 11 11 11
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:8:5) 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

ses encrypt key <hexadecimal> ase encrypt key <hexadecimal> ase encrypt key <hexadecimal> ase encrypt key <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. As the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Beach byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Beach byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Beach byte is represented by a single character. Clears the screen. Clears the screen. Credentials  Clears the screen. Credentials feet byte spaces. Beach byte is represented by a single character. Restores the default feet protocol as 'TCP'.  default protocol as Restores the default protocol as 'TCP'.  default top keep alive Beach byte inneout. Removes the connect unnel AES decrypt key. Removes the connect unnel AES decrypt key. Removes the remote port used to establish tunnel connectons. Removes the remote port used to establish tunnel connectons. Removes the spaces. Removes the connect mode tunneling. Protocol space. Protocol top Uses SSI protocol for connect mode tunneling. Protocol top Uses SSI protocol for connect mode tunneling. Pr</hexadecimal></hexadecimal></hexadecimal></hexadecimal>		
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*12:2abc Note that quotes must enclose the value if it contains spaces.  Sets the connect funnel AES encrypt key 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  cirsom  Clears the screen.  Credentials <text> Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  no aes decrypt key no aes encrypt key Removes the connect tunnel AES decrypt key. no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connect tone the selection.  Removes the remote port used to establish tunnel connect tone to the selection.  Removes the remote port used to establish tunnel to pool to use the selection.  Removes the remote port used to establish tunnel connect to the part of the selection.  Removes the remote port used to establish tunnel connect to the part of the selection.  Removes the VIP name.  Sots the remote port to use for connect mode tunneling.  Protocol ssh Uses SSH protocol for connect mode tunneling.  Protocol top Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol top Uses TCP protocol (with IAC) for connect mode tunneling.  Protocol top uses TCP protocol (with AES encryption for connect mode tunneling.  Protocol udp aes  Show Shows the current configuration.  Show is show is the current configuration.</text>		Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics  cirsorn  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 top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  no aes decrypt key  Removes the connect tunnel AES decrypt key.  no credentials  Clears the RSA/DSA certificate selection.  no port  Removes the connect unnel AES encrypt key.  no credentials  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no ssh username  no top keep alive  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  No vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSL protocol for connect mode tunneling.  protocol top  Uses TCP protocol for connect mode tunneling.  protocol top uses TCP protocol (with AES encryption for connect mode tunneling.  protocol dep  protocol dep  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
cliscrn  Clears the screen.  credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the remote port used to establish tunnel connections.  no sth username  Removes the remote port used to establish tunnel connections.  so ssh username  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssp user scheme to post to use for connect mode tunneling.  Uses TCP 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 tcp uses TCP protocol for connect mode tunneling.  protocol udp  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show uses the current configuration.  Show the current configuration.  Show bistory  CLI session.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connect tunnel AES decrypt key.  no aes encrypt key  Removes the connect tunnel AES decrypt key.  no aes encrypt 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 SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  vnumber&gt;  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSL protocol for connect mode tunneling.  protocol top  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tep aes  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show  Show she current configuration.  Displays the last 20 commands entered during the current CLI session.</text>	auto show statistics	show connection statistics
default protocol  default trop keep alive  default trop keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Ro aes encrypt key  Removes the connect tunnel AES encrypt key.  Ro 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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the VIP name.  Disables the connect mode TCP keep alive timeout.  Ro vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roundber> Sets the remote port to use for connect mode tunneling.  rotocol 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 tep aes  Uses TOP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 tep aes  Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  Protocol udp  Uses UDP protocol or connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp aes  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.	credentials <text></text>	
exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  no top keep alive Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp Uses UDP protocol (with AES encryption for connect mode tunneling.  protocol udp Shows Bows Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	default protocol	Restores the default protocol as "TCP".
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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> Sets the remote port to use for connect mode tunneling.  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 IAC) for connect mode tunneling.  protocol telnet Uses UDP protocol (with IAC) for connect mode tunneling.  protocol 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.	default tcp keep alive	· ·
neling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no aes encrypt key Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  No top keep alive Disables the connect mode TCP keep alive timeout.  No vip name Removes the VIP name Removes the VIP name  Sets the remote port to use for connect mode tunneling. <a href="mailto:rnumber">rnumber</a> Uses SSH protocol for connect mode tunneling.  protocol ssh 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 UDP protocol for connect mode tunneling.  protocol 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.	exit	Exits to the next higher level.
no aes 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.  Removes the VIP name.  Port <number> Sets the remote port to use for connect mode tunneling.  rotocol ssh Uses SSH protocol for connect mode tunneling.  Protocol tcp Uses TCP protocol for connect mode tunneling.  Protocol telnet Uses TCP protocol (with IAC) for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.</number>	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp  Uses UDP protocol with AES encryption for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Shows the current configuration.  Show history  Displays the last 20 commands entered during the current CLI session.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  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.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  Sets the remote port to use for connect mode tunneling.  no top keep alive  Uses SSH protocol for connect mode tunneling.  protocol ssh  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  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.</number>	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  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.  Protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP 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.</number></number>	no port	
no vip name  Removes the VIP name.  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP 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.	no ssh username	Removes the SSH user name.
port <number></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
cnumber> = number of the port to use.   protocol ssh	no vip name	Removes the VIP name.
protocol ssl  Dises SSL protocol for connect mode tunneling.  Dises TCP protocol for connect mode tunneling.  Dises TCP protocol with AES encryption for connect mode tunneling.  Dises TCP protocol with AES encryption for connect mode tunneling.  Dises Telnet protocol (with IAC) for connect mode tunneling.  Dises UDP protocol for connect mode tunneling.  Dises 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.	port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
protocol tcp protocol tcp aes 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.  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.	protocol ssh	Uses SSH 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.  protocol udp  protocol udp aes  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.	protocol ssl	
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  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.	protocol tcp	Uses TCP protocol for connect mode tunneling.
ing.  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.	protocol tcp aes	
protocol udp aes  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.	protocol telnet	1.
tunneling.  show Shows the current configuration.  show history Displays the last 20 commands entered during the current CLI session.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the current CLI session.	protocol udp aes	
CLI session.	show	Shows the current configuration.
show statistics show connection statistics	show history	
	show statistics	show connection statistics

ssh username <text></text>	Sets the SSH user name for use when establishing tun-
SSII username (toxi)	neling connections
	with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and
Top Reep alive Millingecords	sets the timer.
	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:7:5) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
and domint key, they adeaimely	<text> = IP address or host name of the remote host. Sets the connect typical AES depret typically with up to 16.</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
and domination to it.	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
accounters (noxudocimus)	bytes.
	Each byte is represented by two adjacent hex digits.
	Bytes may run together or be separated by optional punctuation:
	123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep
· ·	alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc
	Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc-
aes decrypt key <hexadecimal></hexadecimal>	Sets the connect tunnel AES decrypt key with up to 16 bytes.
address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.</text>
host 5 (tunnel-connect-host:6:5) level commands	
write	Stores the current configuration in permanent memory.
vip name <text></text>	Sets the VIP name.
vip enable	Makes connections using the VIP name.
vip disable	Makes connections using the specified Address.
validate certificate enable	Requires verification of the server certificate when connecting.
validate certificate disable	Skips verification of the server certificate when connecting.
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.

	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:5:5) 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>	0 1 4 4 004/004 477 4 1 4 4 001
	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:4:5) 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 <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
aes encrypt key <hexadecimal></hexadecimal>	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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:3:5) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:2:5) 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
aes decrypt key <i>Chexadechnai&gt;</i>	bytes.
	Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-
	tuation:
	123ABC "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
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16
aco chorypt key text stext?	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.

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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:1:5) 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

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (config-host:5) 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.
write host 6 (tunnel-connect-host:16:6) level commands	Stores the current configuration in permanent memory.
- 12	Sets the remote host to establish tunneling connections with.
host 6 (tunnel-connect-host:16:6) 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>
host 6 (tunnel-connect-host:16:6) 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.</text>
host 6 (tunnel-connect-host:16:6) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-</text>
host 6 (tunnel-connect-host:16:6) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.</text>
host 6 (tunnel-connect-host:16:6) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
host 6 (tunnel-connect-host:16:6) level commands address <text>  aes decrypt key <hexadecimal></hexadecimal></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</text>

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 45 second connect mode TCP keep alive timeout.
Exits to the next higher level.
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 remote port used to establish tunnel connections.
Removes the SSH user name.
Disables the connect mode TCP keep alive timeout.
Removes the VIP name.
Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
Skips verification of the server certificate when connecting.
Requires verification of the server certificate when connecting.
necting.
Makes connections using the specified Address.

write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:15:6) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vin onable	Makes as a section at the MD is a sec-
vip enable	Makes connections using the VIP name.
vip enable vip name <text></text>	Makes connections using the VIP name.  Sets the VIP name.
vip name <text> write</text>	-
vip name <text></text>	Sets the VIP name.
vip name <text> write</text>	Sets the VIP name.
vip name <text> write host 6 (tunnel-connect-host:14:6) level commands</text>	Sets the VIP name.  Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
vip name <text> write host 6 (tunnel-connect-host:14:6) level commands address <text></text></text>	Sets the VIP name.  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</text>
vip name <text> write host 6 (tunnel-connect-host:14:6) level commands address <text>  aes decrypt key <hexadecimal></hexadecimal></text></text>	Sets the VIP name.  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</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:13:6) level commands	
address <text></text>	Sets the remote host to establish tunneling connections with.
and descriptions because the standard	<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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling.
	<number> = number of the port to use.</number>

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.
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> tcp keep alive <milliseconds></milliseconds></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and</text>
top keep diive aminiseeonas	sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:12:6) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	vip disable	Makes connections using the specified Address.
Stores the current configuration in permanent memory.  host 6 (unnel-connect-host11:6) level commands  address < text>  Sets the remote host to establish tunneling connections with.    Sets the connect tunnel AES decrypt key with up to 16 bytes.	vip enable	Makes connections using the VIP name.
Sets the remote host to establish tunneling connections with.   <a 12="" 12.3a,="" 3a="" <fext="" aes="" bc="" bc"="" contains="" decrypt="" enclose="" href="https://dx.com/dx.&lt;/td&gt;&lt;td&gt;vip name &lt;text&gt;&lt;/td&gt;&lt;td&gt;Sets the VIP name.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Sets the remote host to establish tunneling connections with.    clext&gt; = IP address or host name of the remote host.     clext&gt; = 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.&lt;/td&gt;&lt;td&gt;write&lt;/td&gt;&lt;td&gt;Stores the current configuration in permanent memory.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;with.   &lt;text&gt; = IP address or host name of the remote host.   aes decrypt key &lt;hexadecimal&gt; Sets the connect tunnel AES decrypt key with 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.="" text="" that="" the="" value=""> Sets the connect tunnel AES decrypt key 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> Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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 <fext> Sets the connect tunnel AES encrypt key 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 text <fext> Sets the connect tunnel AES encrypt key 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   cliest the RSA/DSA certificates by name for the SSL client.   default protocol Restores the default protocol as "TCP".   default protocol Restores the remote host address used to establish</fext></fext></hexadecimal></a>	host 6 (tunnel-connect-host:11:6) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puncturation: 123ABC '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.  Sets the connect tunnel AES encrypt key 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 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 and the properties of the properties of the set of the properties of</text>	address <text></text>	with.
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 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.  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 protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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.</text>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  no address Removes the remote host address used to establish tunneling connections.  no aes decrypt key Removes the connect tunnel AES decrypt 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 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.  Disables the connect mode TCP keep alive timeout.</text></text>	aes decrypt key text < text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port 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.  Disables the connect mode TCP keep alive timeout.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 remote port used to establish tunnections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	default protocol	Restores the default protocol as "TCP".
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 encrypt key. Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name. Disables the connect mode TCP keep alive timeout.	default tcp keep alive	· ·
neling connections.  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 remote port used to establish tunnel connections. Removes the SSH user name. Disables the connect mode TCP keep alive timeout.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
no ssh username Removes the SSH user name.  no tcp keep alive Disables the connect mode TCP keep alive timeout.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive Disables the connect mode TCP keep alive timeout.	no port	
	no ssh username	Removes the SSH user name.
no vip name Removes the VIP name.	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
	no vip name	Removes the VIP name.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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:

validate certificate disable	Skips verification of the server certificate when connect-
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
110 4441000	neling connections.
no address	Removes the remote host address used to establish tun-
exit	alive timeout.  Exits to the next higher level.
default tcp keep alive	Restores the default 45 second connect mode TCP keep
default protocol	client.  Restores the default protocol as "TCP".
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL
clrscrn	Clears the screen.
auto show statistics	show connection statistics
add dhorypt rey text Clexis	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.
aes encrypt key text < <i>text</i> >	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

l"	וחת
validate certificate enable	ng. Requires verification of the server certificate when con-
	ecting.
vip disable M	Makes connections using the specified Address.
vip enable M	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:9:6) level commands	
	Sets the remote host to establish tunneling connections
	vith. htext> = IP address or host name of the remote host.
	Sets the connect tunnel AES decrypt key with up to 16
b	ytes.
	Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-
tu	uation:
	23ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains
	paces.
I	Sets the connect tunnel AES decrypt key with up to 16
l	ytes. Each byte is represented by a single character.
	lote that quotes must enclose the value if it contains
-	paces.
	Sets the connect tunnel AES encrypt key with up to 16 ytes.
	each byte is represented by two adjacent hex digits.
	Sytes may run together or be separated by optional punc-
1	uation: 23ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc
N	lote that quotes must enclose the value if it contains
	paces.
	Sets the connect tunnel AES encrypt key with up to 16 ytes.
E	ach byte is represented by a single character.
	lote that quotes must enclose the value if it contains paces.
	how connection statistics
clrscrn	Clears the screen.
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL
	lient.
·	Restores the default protocol as "TCP".
	Restores the default 45 second connect mode TCP keep live timeout.
exit E	xits to the next higher level.
	Removes the remote host address used to establish tun- eling 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 C	Clears the RSA/DSA certificate selection.
	Removes the remote port used to establish tunnel con- ections.
no ssh username	Removes the SSH user name.

Disables the segment mode TCD keep alive times at
Disables the connect mode TCP keep alive timeout.
Removes the VIP name.
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.
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>
Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
Skips verification of the server certificate when connecting.
Requires verification of the server certificate when connecting.
Makes connections using the specified Address.
Makes connections using the VIP name.
Sets the VIP name.
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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.

	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:7:6) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel con-

	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:5:6) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel con-
	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:4:6) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun-

	neling connections with other devices.
	<text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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
aes decippi key (nexadecimal)	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:2:6) 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
aes encrypt key <hexadecimal></hexadecimal>	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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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  sh username < text>  Sets the SSH user name for use when establishing tun neling connections with other devices. <text> = SSH user name.  tcp keep alive &lt; milliseconds&gt;  Enables TCP keep alive for connect mode tunneling ar 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.  vip disable  Makes connections using the specified Address.  vip enable  vip name &lt; text&gt;  Sets the VIP name.  vip name &lt; text&gt;  Sets the VIP name.  Stores the current configuration in permanent memory.  itost 6 (tunnel-connect-host:1:6) level commands  address &lt; text&gt;  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 put tuation:  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.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Sets the connect tunnel AES decrypt key with up to 16 bytes.</text></milliseconds></text>
sets the timer. <pre> <pre></pre></pre>
validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Write  Stores the current configuration in permanent memory.  **Tost 6 (tunnel-connect-host:1:6) level commands**  address < text>  Sets the remote host to establish tunneling connections with. <a 12="" 12,3a,bc="" 12.3a.bc="" 12:3a:bc="" 3a="" <text="" aes="" bc"="" contains="" decrypt="" enclose="" href="https://www.nemotesconnect-host-nost-nost-nost-nost-nost-nost-nost-n&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;vip disable  vip enable  vip enable  vip name &lt;text&gt;  Sets the VIP name.  write  Stores the current configuration in permanent memory.  host 6 (tunnel-connect-host:1:6) level commands  address &lt;text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = 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 put tuation:  123ABC " if="" it="" key="" must="" note="" quotes="" spaces.="" text="" that="" the="" value="">  Sets the connect tunnel AES decrypt key with up to 16 bytes.</a>
vip enable  vip name <text>  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 6 (tunnel-connect-host:1:6) 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 put tuation:  123ABC "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.</text></text></text></text>
vip name <text>  Sets the VIP name.  Write  Stores the current configuration in permanent memory.  host 6 (tunnel-connect-host:1:6) 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 put tuation:  123ABC "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.</text></text></text></text>
write  Stores the current configuration in permanent memory.  host 6 (tunnel-connect-host:1:6) 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 put tuation:  123ABC "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 &lt; text&gt;  Sets the connect tunnel AES decrypt key with up to 16 bytes.</text>
host 6 (tunnel-connect-host:1:6) 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 put tuation:  123ABC "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 &lt; text&gt;  Sets the connect tunnel AES decrypt key with up to 16 bytes.</text>
address <text>  Sets the remote host to establish tunneling connections with.  <text> = IP address or host name of the remote host.  aes decrypt key <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 put tuation:  123ABC "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.</text></hexadecimal></text></text>
with. <text> = IP address or host name of the remote host.  aes decrypt key <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 put tuation:  123ABC "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.</text></hexadecimal></text>
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional put tuation: 123ABC "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.</text>
bytes.
Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.
aes encrypt key <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 put tuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains spaces.</hexadecimal>
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</text>
spaces.
auto show statistics show connection statistics
auto show statistics show connection statistics
auto show statistics  clrscrn  credentials < text>  show connection statistics  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL
auto show statistics  clrscrn  Clears the screen.  credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.</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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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

this host is selected on the login connect menu.    ctext> = IP address.   Sets the remote port used to connect to 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.  Sets the protocol to Telnet.  Sets the termote port verb to set used.  Solomous tell paddress.  Sets the remote port used to connect to the host.   Sets the termote port used to connect to the host.  Sets the remote port used to connect to the host.  Sets the current configuration. Sets the username for logging into the host via SSH. <	name <text></text>	
Clears the SSH username associated with the host.	no name	Clears the name of the host.
protocol ssh protocol telnet Sets the protocol to SSH. Sets the IP address of the remote host to connect to wher this host is selected on the login connect menu.    <ekzb =="" address.="" ip="" td=""  =""  <=""><td>no remote address</td><td>Clears the remote address of the host.</td></ekzb>	no remote address	Clears the remote address of the host.
protocol telnet  Sets the protocol to Telnet.  Sets the IP address of the remote host to connect to wher this host is selected on the login connect menu. <text> = IP address.  femote port <number> Sets the remote port used to connect to the host.  <number> = port to be used.  Show  Displays the last 20 commands entered during the current CLI session.  Show history  Sets the username for logging into the host via SSH.  <text> = Username.  Stores the current configuration in permanent memory.  Nost 7 (tunnel-connect-host:16:7) level commands address <text>  Sets the username for logging into the host via SSH.  <text> = Username.  Stores the current configuration in permanent memory.  Nost 7 (tunnel-connect-host:16:7) 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 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 qu</text></text></text></text></text></number></number></text>	no ssh username	Clears the SSH username associated with the host.
Sets the IP address of the remote host to connect to wher this host is selected on the login connect menu.    remote port <number>   sets the remote port used to connect to the host.   show Displays the current configuration.   show history Displays the last 20 commands entered during the current CLI session.   show history Sets the remote host to last 20 commands entered during the current CLI session.   show show history Sets the username for logging into the host via SSH.   vitext&gt; = username.   write Stores the current configuration in permanent memory.   host 7 (tunnel-connect-host16:7) level commands   address <text> Sets the remote host to establish tunneling connections with.   vitex = IP address or host name of the remote host.   aes decrypt key <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 two adjacent hex digits. Bytes in a presented by two adjacent hex digits.   Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12.3A, BC 12.3a bc 12:3a bc   aes encrypt key <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 opti</hexadecimal></text></hexadecimal></text></number>	protocol ssh	Sets the protocol to SSH.
this host is selected on the login connect menu.    Itemote port < number>   Sets the remote port used to connect to the host.	protocol telnet	Sets the protocol to Telnet.
cnumber> = port to be used.   show	remote address <text></text>	selected on the login connect menu.
Show history  Displays the last 20 commands entered during the current CLI session.  Sets the username for logging into the host via SSH. <a href="text">text</a>	remote port <number></number>	
Sets the username <text> Sets the username for logging into the host via SSH. <text> = username.  write Stores the current configuration in permanent memory.  host 7 (tunnel-connect-host-16:7) 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.  Bach byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  auto show statistics  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.</text></text></text></text></text>	show	Displays the current configuration.
write Stores the current configuration in permanent memory.  host 7 (tunnel-connect-host:16:7) 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.  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 gootes must enclose the value if it contains spaces.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	show history	Displays the last 20 commands entered during the current CLI session.
Sets the remote host to establish tunneling connections with.   <text> = IP address or host name of the remote host.    </text>	ssh username <text></text>	_ = =
Sets the remote host to establish tunneling connections with.    Acetax		Stores the current configuration in permanent memory.
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.  Clears the screen.  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.</text>	host 7 (tunnel-connect-host:16:7) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.  auto show statistics show connection statistics clrscm Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.	address <text></text>	with.
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.  Selects the RSA/DSA certificates by name for the SSL client.	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Selects the RSA/DSA certificates by name for the SSL client.</text>	aes decrypt key text <text></text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
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.</text>	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
clrscrn Clears the screen.  credentials <text> Selects the RSA/DSA certificates by name for the SSL client.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.</text>	auto show statistics	show connection statistics
client.	clrscrn	Clears the screen.
default protocol Restores the default protocol as "TCP".	credentials <text></text>	
	default protocol	Restores the default protocol as "TCP".

default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:15:7) 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.

protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	neling connections.  Removes the connect tunnel AES decrypt key.
no address	Removes the remote host address used to establish tun-
exit	alive timeout.  Exits to the next higher level.
default tcp keep alive	Restores the default 45 second connect mode TCP keep
default protocol	Restores the default protocol as "TCP".
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL client.
clrscrn	Clears the screen.
auto show statistics	show connection statistics
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.
	123ABC "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 <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:
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.
	Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

show   Shows the current configuration.	protocol udp aes	Uses UDP protocol with AES encryption for connect mode
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. <a 12="" 12.3a.bc="" 12:3a:bc="" 3a="" <text="" aes="" bc"="" contains="" decrypt="" enclose="" href="https://doi.org/10.1001/journal-connections-con&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;-&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;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.           &lt;p&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Sets the SSH user name for use when establishing tunneling connections with other devices.    tcp keep alive &lt; milliseconds&gt;   tcp keep alive &lt; milliseconds&gt;   tcp keep alive &lt; milliseconds&gt;    &lt;/td&gt;&lt;td&gt;show history&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;neling connections with other devices. &lt;text&gt; = SSH user name.  top keep alive &lt;milliseconds&gt; Enables TCP keep alive for connect mode tunneling and sets the timer.  milliseconds&gt; = 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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name &lt;text&gt; Sets the VIP name.  Vip name.  Stores the current configuration in permanent memory.  Nost 7 (tunnel-connect-host-14-7) level commands  address &lt;text&gt;  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = IP address or host name of the remote host.  Sets the remote host to establish tunneling connections with.  &lt;text&gt; = 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.  aes encrypt key &lt;hexadecimal&gt;  Sets the connect tunnel AES encrypt key 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 12.3&lt;/td&gt;&lt;td&gt;show statistics&lt;/td&gt;&lt;td&gt;show connection statistics&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;sets the timer.  &lt;pre&gt;&lt;/td&gt;&lt;td&gt;ssh username &lt;text&gt;&lt;/td&gt;&lt;td&gt;neling connections with other devices.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  vip name &lt;text&gt; Sets the VIP name.  vip name &lt;text&gt; Sets the VIP name.  Stores the current configuration in permanent memory.  host 7 (tunnel-connect-host:14:7) level commands  address &lt; text&gt;  Sets the remote host to establish tunneling connections with.  &lt;ext&gt;&lt;ext&gt; = 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 " if="" it="" key="" must="" note="" quotes="" spaces.="" text="" that="" the="" value="">  Sets the connect tunnel AES decrypt key 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>  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  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. N</hexadecimal></a>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  vip name <text>  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 7 (tunnel-connect-host:14:7) 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.  aes encrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 by</hexadecimal></text></text></text>	validate certificate disable	l. ·
vip enable  vip name <text>  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  It contains the connect-host:14:7) 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.  aes decrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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.  As the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC*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.  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  clears the screen.</text></text></hexadecimal></text></text></text>	validate certificate enable	
virite  Stores the VIP name.  Stores the current configuration in permanent memory.  Inst 7 (tunnel-connect-host:14:7) 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 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.</text>	vip disable	Makes connections using the specified Address.
write Stores the current configuration in permanent memory.    Sets the remote host to establish tunneling connections with.	vip enable	Makes connections using the VIP name.
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 decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.</text></text>	vip name <text></text>	Sets the VIP name.
address <text>  Sets the remote host to establish tunneling connections with.  <text>= IP address or host name of the remote host.  aes decrypt key <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.  Sets the connect tunnel AES decrypt key 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.</hexadecimal></text></text>	write	Stores the current configuration in permanent memory.
with. <text> = IP address or host name of the remote host.  aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.</text></hexadecimal></text>	host 7 (tunnel-connect-host:14:7) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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>  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  auto show statistics Clears the screen.</text></hexadecimal></text>	address <text></text>	with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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  clrscrn  Clears the screen.</text></hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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  clrscrn  Clears the screen.</text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
clrscrn Clears the screen.	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
	auto show statistics	show connection statistics
credentials <text> Selects the RSA/DSA certificates by name for the SSL</text>	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:13:7) 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>
Sets the connect tunnel AES decrypt key with up to 16
bytes.
Each byte is represented by two adjacent hex digits.
Bytes may run together or be separated by optional punctuation:
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 punc-
tuation:
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 45 second connect mode TCP keep alive timeout.
Exits to the next higher level.
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 remote port used to establish tunnel connections.
Removes the SSH user name.
Disables the connect mode TCP keep alive timeout.
Removes the VIP name.
Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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

protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:12:7) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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 top aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  show  Show the current configuration.  Show thistory  Displays the last 20 commands entered during the current configuration and tunneling.  Show statistics  show connection statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.  stavt > SSH user name for use when establishing tunneling connections  with other devices.  stavt > SSH user name.  top keep alive <milliseconds>  estate to time.  williseconds&gt; estate the time.  williseconds&gt; estate the time.  williseconds&gt; estate the time.  willidate certificate disable  Skips verification of the server certificate when connecting.  wip disable  Makes connections using the VIP name.  wip name   wite Makes connections using the VIP name.  wite Stores the current configuration in permanent memory.  Nost 19 Audition of the server certificate with the connections with the virtual part of the server certificate with connecting.  With Stores the current configuration in permanent memory.  Nost 19 Audition of the server certificate when connecting.  Sets the VIP name.  With Stores the current configuration in permanent memory.  Nost 19 Audition of the server certificate when connecting the virtual part of the termote 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 123A</milliseconds>		
ing.  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Show Show with current configuration.  Show 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.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect unde tunneling and sets the timer.  - williseconds = 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.  Walkes connections using the specified Address.  vip disable  vip name   Makes connections using the VIP name.  vip amble  Makes connections using the VIP name.  vip ame   Sets the VIP name.  Stores the current configuration in permanent memory.  host 7 (tunnel-connect-host-10:7) level commands  address   Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC *12 2.3 a.b C 12.3 a.b C 1</milliseconds>	protocol tcp aes	
Uses UDP protocol with AES encryption for connect mode tunnelling.	protocol telnet	l.
tunneling.	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.  - dext>	protocol udp aes	
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices.    tcp keep alive <milliseconds></milliseconds>	show history	
nelling connections   with other devices.   etaxl= SSH user name.	show statistics	show connection statistics
sets the timer.  \text{\text{milliseconds}} = timer value, in milliseconds.  \text{validate certificate disable}  \text{Skips verification of the server certificate when connecting.}  \text{validate certificate enable}  \text{Requires verification of the server certificate when connecting.}  \text{vip disable}  \text{Makes connections using the specified Address.}  \text{vip enable}  \text{vip enable}  \text{Makes connections using the VIP name.}  \text{vip name \text{text}}  \text{Sets the VIP name.}  \text{write}  \text{Stores the current configuration in permanent memory.}  \text{Nost 7 (tunnel-connect-host:10:7) level commands}  \text{address} < \text{text} > \text{Sets the current configuration in permanent memory.}  \text{Nost 7 (tunnel-connect-host:10:7) level commands}  \text{address} < \text{text} > \text{IP address or host name of the remote host.}  \text{Sets the remote host to establish tunneling connections with.}  \text{\text} = IP address or host name of the remote host.}  \text{Sets the connect tunnel AES decrypt key with up to 16 bytes.}  \text{Each byte is represented by two adjacent hex digits.}  \text{Bytes may run together or be separated by optional punctuation:}  \text{12.3ABC "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.}  \text{aes encrypt key <hexadecimal>}  \text{Sets the connect tunnel AES decrypt key with up to 16 bytes.}  \text{Each byte is represented by two adjacent hex digits.}  \text{Bytes may run together or be separated by optional punctuation:}  \text{12.3ABC "12.3A,BC 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.}  \text{aes the connect tunnel AES encrypt key with up to 16 bytes.}  \text{Bach byte is represented by two adjacent hex digits.}  \text{Bytes may run together or be separated by optional punctuation:}  \text{12.3ABC "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.}  Act bytes.</hexadecimal>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  host 7 (tunnel-connect-host:10:7) 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 7 (tunnel-connect-host:10:7) 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate disable	I. ·
vip enable  vip name <text> Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 7 (tunnel-connect-host:10:7) 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 7 (tunnel-connect-host:10:7) 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Stes the current current permanent memory.   Stes the current current current permanent memory.   Stes the current current permanent memory.   Stes the current current current permanent memory.   Stes the current current current permanent memory.   Stes the current current	vip enable	Makes connections using the VIP name.
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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vip name <text></text>	Sets the VIP name.
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 optional punctuation: 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.</text>	write	Ctores the current configuration in normanant mamoru
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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	Witte	Stores the current configuration in permanent memory.
aes decrypt key <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.  Sets the connect tunnel AES decrypt key 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</hexadecimal>	- 12	Stores the current configuration in permanent memory.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	host 7 (tunnel-connect-host:10:7) level commands	Sets the remote host to establish tunneling connections with.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	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>
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	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.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	host 7 (tunnel-connect-host:10:7) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	host 7 (tunnel-connect-host:10:7) level commands address <text>  aes decrypt key <hexadecimal>  aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:9:7) level commands	S
address <text></text>	Sets the remote host to establish tunneling connections with.
	<pre><text> = IP address or host name of the remote host.</text></pre>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:8:7) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

vip name <text>         Makes connections using the VIP name.           vip name <text>         Sets the VIP name.           vip name <text>         Sets the VIP name.           storest the current configuration in permanent memory.         Sets the current configuration in permanent memory.           drows / (tunnel-connect-host.77) level commands         Sets the connect tunnel AES decrypt key with up to 16 bytes.           aces decrypt key &lt;-hexadecimal&gt;         Sets the connect tunnel AES decrypt key with up to 16 bytes.           Each byte is represented by two adjacent hex digits.         Bytes may run together or be separated by optional punctuation:           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.           aes encrypt key &lt;-hexadecimal&gt;         Sets the connect tunnel AES encrypt key with up to 16 bytes.           Each byte 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></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Inst17 (tunnel-connect-host:77) level commands   address < text>	vip enable	
address < text>  Sets the remote host to establish tunneling connections with. <text>= IP address or host name of the remote host.  ✓text&gt; = 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.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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 unnel AES encrypt key 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 unnel AES encrypt key mith 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 unnel AES encrypt key 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 unnel AES encrypt key and the present that quotes must enclose the value if it contains spaces.  Sets the connect unnel AES encrypt key and the present quotes must enclo</text>	vip name <text></text>	Sets the VIP name.
address <text> Sets the remote host to establish tunneling connections with.  <text>= IP address or host name of the remote host.  dext&gt; = 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 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 and the properties of the set of the next higher level.  Restores the default protocol as 'TCP'. default top top the properties of the next higher level.  Removes the remote host address used to establish tunneling connections.  No assencypt key</text></text>	write	Stores the current configuration in permanent memory.
with.	host 7 (tunnel-connect-host:7:7) level commands	
bytes. 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	address <text></text>	with.
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 character. Note that quotes must enclose the value if it contains spaces.  auto show statistics  show connection 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".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  no aes encrypt key  Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.  Removes the remote host address used to establish tunneling connections.  no port  Removes the connect tunnel AES encrypt key.  Removes the connect tunnel AES encrypt key.</text>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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 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".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  no aeddress Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  no aes encrypt key Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  no port 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 to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text></text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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> Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  no tcp keep alive Disables the connect mode TCP keep alive timeout.</text>	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
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".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit to the next higher level.  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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnections.  Removes the remote port used to establish tunnel connections.  Removes the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text>	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 encrypt key.  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnections.  Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	default protocol	Restores the default protocol as "TCP".
no address  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	default tcp keep alive	
neling connections.  no aes decrypt key 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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
no ssh username Removes the SSH user name.  no tcp keep alive Disables the connect mode TCP keep alive timeout.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive Disables the connect mode TCP keep alive timeout.	no port	i i
	no ssh username	Removes the SSH user name.
no vip name Removes the VIP name.	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
	no vip name	Removes the VIP name.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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:

validate certificate disable	Skips verification of the server certificate when connect-
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port <number></number>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
ino addiess	neling connections.
no address	Removes the remote host address used to establish tun-
exit	alive timeout.  Exits to the next higher level.
default top keep alive	Restores the default 45 second connect mode TCP keep
default protocol	client.  Restores the default protocol as "TCP".
credentials <text></text>	Selects the RSA/DSA certificates by name for the SSL
clrscrn	Clears the screen.
auto show statistics	show connection statistics
add dhorypt rey text stexts	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <text></text>	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

	ing.
validate certificate enable	Requires verification of the server certificate when con-
validate estimolie estable	necting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:5:7) 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 punc-
	tuation:
	123ABC "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 punc-
	tuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.

no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:4:7) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer.

	<milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:3:7) level comr	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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel con-
	· · · · · · · · · · · · · · · · · · ·

	nections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:2:7) 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>	Sets the connect tunnel AES decrypt key 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:1:7) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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. <a href="text"><a 12="" 12,3a,bc="" 12.3a.bc="" 12:3a:bc="" 3a="" bc"="" contains="" enclose="" href="text&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;write&lt;/td&gt;&lt;td&gt;Stores the current configuration in permanent memory.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;host 8 (tunnel-connect-host:16:8) level commands&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;address &lt;text&gt;&lt;/td&gt;&lt;td&gt;Sets the remote host to establish tunneling connections with.  &lt;text&gt; = IP address or host name of the remote host.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;aes decrypt key &lt;hexadecimal&gt;&lt;/td&gt;&lt;td&gt;Sets the connect tunnel AES decrypt key with 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="" must="" note="" quotes="" spaces.<="" td="" that="" the="" value=""></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc
and and the state of the state	bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:
address <text>  aes decrypt key <hexadecimal></hexadecimal></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</text>
host 8 (tunnel-connect-host:15:8) level commands	Outs the provide head to entail P. L. C.
write	Stores the current configuration in permanent memory.
vip name <text></text>	Sets the VIP name.
vip enable	Makes connections using the VIP name.
vip disable	Makes connections using the specified Address.
validate certificate enable	Requires verification of the server certificate when connecting.
validate certificate disable	Skips verification of the server certificate when connecting.
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.

	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:14:8) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:13:8) 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.
<u>'</u>	

	Bytes may run together or be separated by optional punctuation: 123ABC "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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:12:8) 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 top keep alive	Restores the default 45 second connect mode TCP keep
default top keep alive	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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> aes decrypt key text <text></text></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.  Sets the connect tunnel AES decrypt key 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</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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.

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>
Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
Skips verification of the server certificate when connecting.
Requires verification of the server certificate when connecting.
Makes connections using the specified Address.
Makes connections using the VIP name.
Sets the VIP name.
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>
<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>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:9:8) 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>
Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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 45 second connect mode TCP keep alive timeout.
Exits to the next higher level.
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 remote port used to establish tunnel connections.
Removes the SSH user name.
Disables the connect mode TCP keep alive timeout.
Removes the VIP name.
Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.

protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:8:8) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

with.	host 8 (tunnel-connect-host:7:8) 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 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 optional punctuation:  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.  Clears the screen.  Clears the default protocol as "TCP".  Restores the default to second connect mode TCP keep alive timeout.  Exists to the next higher level.  Removes the remote host address used to establish tunneling connections.  no aes encrypt key  no credentials  no port  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote host address used to establish tunneling connections.  Permoves the connect nunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote host	address <text></text>	_
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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 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 RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key. Removes the connect nunnel AES encrypt key.  Removes the connect nunnel AES encrypt key.  Clears the RSA/DSA certificate selectio		<text> = IP address or host name of the remote host.</text>
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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 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 clrscm Clears the screen.  Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address Removes the remote host address used to establish tunneling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no credentials Clears the RSA/DSA certificates election.  Removes the remote port 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 SSH user name.  No top keep alive Disables the connect mode TCP keep alive timeout.  Removes the SSH user name.  Removes the SSH user name.  Removes the SPH user name.  Removes the port to use for connect mode tunneling.  Note that quotes must enclose the value if it contains spaces.</hexadecimal>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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. 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 protocol as "TCP". Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level. 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 encrypt key. Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunneling connections. Removes the remote port used to establish tunnel port encent encent</text>	aes decrypt key text < text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
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.  Clears the SA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no port  Removes the SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rounder> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  ¬umber> = number of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.	aes encrypt key text < text>	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunneling transport of the port used to establish tunnel 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.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  Anumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.	auto show statistics	show connection statistics
default protocol  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 connect tunnel AES encrypt key.  Removes the remote port used to establish tunnel on nections.  Removes the remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rounder> = number of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.	clrscrn	Clears the screen.
Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Disas SSH protocol for connect mode tunneling.  Vises SSH protocol for connect mode tunneling.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  In the port of the port to use.  Protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	default protocol	Restores the default protocol as "TCP".
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 remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  enumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	default tcp keep alive	
neling connections.  no aes decrypt 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 remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  port <number>  protocol ssh  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.</number>	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  no vip name  port <number> Sets the remote port to use.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.</number>	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> = number of the port to use.  Uses SSH protocol for connect mode tunneling.  Uses SSL protocol for connect mode tunneling.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Removes the VIP name.  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.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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.	no port	· ·
no vip name  Removes the VIP name.  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 ssh username	Removes the SSH user name.
port <number> 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></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
<pre>conumber = number of the port to use. protocol ssh</pre>	no vip name	Removes the VIP name.
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	Uses SSL protocol for connect mode tunneling.
	protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tep aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol teinet  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Show state our current configuration.  Show the current configuration.  Show statistics  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.  tcp keep alive **rmilliseconds>**  tcp keep alive **emilliseconds>**  Enables TCP keep alive for connect mode tunneling 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.  Vip disable  Makes connections using the VIP name.  Vip p name <text>  Write  Stores the VIP name.  Virunel**  Stores the current configuration in permanent memory.  Total the curre</text>		
ing.  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.  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 name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  **milliseconds&gt; = timer value, in milliseconds.  Validate certificate disable  Skips verification of the server certificate when connecting.  vip disable  Wakes connections using the specified Address.  Vip enable  Vip name <text>  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the current configuration in permanent memory.  **Nost 8 (tunnel-connect-host-6:8) level commands*  address &lt;*text&gt;  Sets the remote host to establish tunneling connections with,  **\text&lt;= 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 12:3a.bc 12:3a.bc Note that quotes must enclose the value if it contains spaces.  aes encrypt key &lt;*hexadecimal&gt;  Sets the connect tunnel AES decrypt key 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 two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC '123ABC '</text></milliseconds>	protocol tcp aes	
protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunnelling.  show  Shows the current configuration.  Displays the last 20 commands entered during the current CLI session.  show statistics  show connection statistics  show connections with other devices.  Sets the SSH user name for use when establishing tunneling connections with other devices name.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  vip disable  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Stores the current configuration in permanent memory.  Notal (tunnel-connects-host-6:8) level commands  address <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Sets the connect unnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC '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 <hexadecimal>  Sets the connect tunnel AES encrypt key 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 op</hexadecimal></text></milliseconds>	protocol telnet	l.
show Shows the current configuration.  Show thistory 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.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the current CLI session.  Show connection statistics  show statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.	protocol udp aes	
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices.  top keep alive <milliseconds>  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  <milliseconds> = timer value, in milliseconds.  Skips verification of the server certificate when connecting.  validate certificate enable  Requires verification of the server certificate when connecting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the specified Address.  vip name <text> Sets the VIP name.  vithe Stores the current configuration in permanent memory.  host 3 (tunnel-connect-host:6:3) 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.  aes encrypt key <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 16 bytes.  Each byte is represented by two adjacent hex 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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></hexadecimal></text></text></text></milliseconds></milliseconds></milliseconds>	show history	
neling connections with other devices. <text> = SSH user name.  tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling 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.  Vip disable  Makes connections using the specified Address.  Vip name <text>  Makes connections using the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 8 (tunnel-connect-host:6:8) level commands  address <text>  Sets the remote 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.  Bach byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *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 <hexadecimal>  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Sets the connect runnel AES encrypt key with up to 16 bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a.bc  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a.bc  Note that quotes must enclose the value if it contains spaces.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC *12 3A BC* 12,3A,BC 12.3a.bc 12:3a.bc  Note that q</hexadecimal></text></te></text></text></milliseconds></milliseconds></text>	show statistics	show connection statistics
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.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 8 (tunnel-connect-host:6:8) level commands  address &lt; text&gt;  Sets the remote host to establish tunneling connections with.  &lt; </milliseconds>	ssh username <text></text>	neling connections with other devices.
validate certificate enable  Requires verification of the server certificate when connecting.  Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Wakes connections using the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Sets the vIP name.  Sets the connections using the VIP name.  Stores the current configuration in permanent memory.  Sets the connect to establish tunneling connections with.     Address A	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name < text>  Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Sets the virrent configuration in permanent memory.  host 8 (tunnel-connect-host:6:8) level commands  address < text>  Sets the remote host to establish tunneling connections with.	validate certificate disable	I. ·
vip enable vip name <text> Sets the VIP name. Sets the VIP name. Stores the current configuration in permanent memory.  Nost 8 (tunnel-connect-host:6:8) 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 optional punctuation: 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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text></text>	validate certificate enable	
vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 8 (tunnel-connect-host:6:8) level commands  address <text>  Sets the remote host to establish tunneling connections with.     Sets the connect tunnel AES decrypt key with up to 16 bytes.   Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.   Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.	vip enable	Makes connections using the VIP name.
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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text>	vip name <text></text>	Sets the VIP name
aes decrypt key <hexadecimal>  Sets the remote host to establish tunneling connections with.  <text> = IP address or host name of the remote host.   aes decrypt key <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> Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text></hexadecimal></text></hexadecimal></text></hexadecimal>	Life transfer warm	octs the vir marie.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 23ABC "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.</text></text>		
aes decrypt key <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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></hexadecimal>	write	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text></text>	write host 8 (tunnel-connect-host:6:8) level commands	Stores the current configuration in permanent memory.  Sets the remote host to establish tunneling connections with.
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  aes encrypt key <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.</text></hexadecimal>	write host 8 (tunnel-connect-host:6:8) level commands address <text></text>	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>
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	write 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.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	write host 8 (tunnel-connect-host:6:8) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	write host 8 (tunnel-connect-host:6:8) level commands address <text> aes decrypt key <hexadecimal> aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

host 8 (tunnel-connect-host:5:8) level commands address <text>  aes decrypt key <hexadecimal>  aes decrypt key text <text>  aes encrypt key <hexadecimal></hexadecimal></text></hexadecimal></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</text>
aes decrypt key <hexadecimal>  aes decrypt key text <text>  aes decrypt key text <text>  aes encrypt key <hexadecimal></hexadecimal></text></text></hexadecimal>	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.</text>
aes decrypt key <hexadecimal>  aes decrypt key text <text>  aes encrypt key <hexadecimal></hexadecimal></text></hexadecimal>	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.</text>
aes decrypt key <hexadecimal>  aes decrypt key text <text>  aes encrypt key <hexadecimal></hexadecimal></text></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.  Sets the connect tunnel AES decrypt key 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 decrypt key text <text> aes encrypt key <hexadecimal></hexadecimal></text>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.
aes encrypt key <hexadecimal></hexadecimal>	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>	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	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".
	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
	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.
	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
protocol ssh	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>

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.
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>  tcp keep alive <milliseconds></milliseconds></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.  Enables TCP keep alive for connect mode tunneling and</text>
top keep alive	sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:4:8) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 < <i>text</i> >	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.

tuation:  123ABC "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 <fext>  Sets the connect tunnel AES decrypt key 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.  auto show statistics clorern Clears the screen.  Clears the screen.  Clears the SA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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 encrypt key.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no sph username Removes the SBH user name.  Disables the connect mode TCP keep alive timeout.</fext>	vip disable	Makes connections using the specified Address.
Stores the current configuration in permanent memory.  Nost 8 (unnel-connect-hosts) level commands address < text>  Sets the remote host to establish tunneling connections with.    Sets the connect tunnel AES decrypt key with up to 16 bytes.     Each byte is represented by two adjacent hex digits.     Bytes may run together or be separated by optional punctuation:   123ABC '12 3A BC '12 3A BC 12	vip enable	Makes connections using the VIP name.
Activation of the remote host to establish tunneling connections with.    Interest   Paddress or host name of the remote host to establish tunneling connections with.   Interest   Paddress or host name of the remote host.	vip name <text></text>	Sets the VIP name.
Sets the remote host to establish tunneling connections with.    clears = IP address or host name of the remote host.     clears = IP address or host name of the remote host.     clears = 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	write	Stores the current configuration in permanent memory.
with.	host 8 (tunnel-connect-host:3:8) level commands	
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional puncturation: 123ABC "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.  Sets the connect tunnel AES encrypt key 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 and the properties of the default protocol as "TCP".  Restores the default as second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the connect tunnel AES decrypt key.  Clears the RSA/DSA certificate selection.  Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel conne</text>	address <text></text>	with.
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 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.  Clears the screen.  Credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  Clear the patient protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 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.</text>	aes decrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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 clrscrn  Clears the screen.  Clears the screen.  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 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  no aes encrypt 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 used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.</text></text>	aes decrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
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.  Clears the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default top keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port 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.  Disables the connect mode TCP keep alive timeout.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
Clears the screen.  Credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 remote port used to establish tunnel port  Removes the remote port used to establish tunnel connections.  Removes the SA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
Selects the RSA/DSA certificates by name for the SSL client.  default protocol Restores the default protocol as "TCP".  default tcp keep alive Restores the default 45 second connect mode TCP keep alive timeout.  exit Exits to the next higher level.  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.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnections.  no ssh username Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	auto show statistics	show connection statistics
client.  default protocol  default tcp keep alive  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exit Exits to the next higher level.  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 remote port used to establish tunnections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	credentials <text></text>	
alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	default protocol	Restores the default protocol as "TCP".
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 encrypt key. Clears the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name. Disables the connect mode TCP keep alive timeout.	default tcp keep alive	·
neling connections.  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 remote port used to establish tunnel connections. Removes the SSH user name. Disables the connect mode TCP keep alive timeout.	exit	Exits to the next higher level.
no aes encrypt key  no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
no port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
no ssh username Removes the SSH user name. Disables the connect mode TCP keep alive timeout.	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive Disables the connect mode TCP keep alive timeout.	no port	
	no ssh username	Removes the SSH user name.
no vip name Removes the VIP name.	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
	no vip name	Removes the VIP name.

port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:2:8) 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:

to show statistics scrn cdentials <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. show connection statistics Clears the SCA/DSA certificates by a case for the SCA
scrn (Cedentials < text>	Clears the screen.
edentials <text></text>	
	Colorto the DCA/DCA contitiontes by page for the CCI
	Selects the RSA/DSA certificates by name for the SSL client.
fault protocol	Restores the default protocol as "TCP".
	Restores the default 45 second connect mode TCP keep alive timeout.
it E	Exits to the next higher level.
	Removes the remote host address used to establish tunneling connections.
aes decrypt key F	Removes the connect tunnel AES decrypt key.
	Removes the connect tunnel AES encrypt key.
credentials	Clears the RSA/DSA certificate selection.
	Removes the remote port used to establish tunnel connections.
ssh username F	Removes the SSH user name.
tcp keep alive	Disables the connect mode TCP keep alive timeout.
vip name F	Removes the VIP name.
	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>
otocol ssh U	Uses SSH protocol for connect mode tunneling.
otocol ssl L	Uses SSL protocol for connect mode tunneling.
otocol tcp U	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.
otocol udp U	Uses UDP protocol for connect mode tunneling.
	Uses UDP protocol with AES encryption for connect mode tunneling.
ow S	Shows the current configuration.
	Displays the last 20 commands entered during the current CLI session.
ow statistics s	show connection statistics
r v	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
S	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
lidate certificate disable	Skips verification of the server certificate when connect-

	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:1:8) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.

no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  protocol ssl  protocol tcp  protocol tcp  protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  protocol udp  protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Show  Shows the current configuration.  Show statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.  **CENTENT SSH user name**  **CENTENT SSH user name**  Sets the SSH user name.
Image: Norm   Image: Norm
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.  protocol telnet Uses Telnet protocol (with IAC) for connect mode tunneling.  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.  Show statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
protocol tcp protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  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 she wistory  Displays the last 20 commands entered during the currence CLI session.  Show statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
protocol tcp aes  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  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 curred CLI session.  Show statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunne ing.  protocol udp  Uses UDP protocol for connect mode tunneling.  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 curre CLI session.  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
ing.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect motunneling.  Show  Shows the current configuration.  Show history  Displays the last 20 commands entered during the current session.  Show statistics  Show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
protocol udp aes  Uses UDP protocol with AES encryption for connect motunneling.  Show  Shows the current configuration.  Displays the last 20 commands entered during the current session.  Show statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
tunneling.  show  Shows the current configuration.  Show history  Displays the last 20 commands entered during the curre CLI session.  show statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
show history  Displays the last 20 commands entered during the curre CLI session.  show statistics  show connection statistics  Sets the SSH user name for use when establishing tunneling connections with other devices.
Show statistics  show connection statistics  ssh username <text>  Sets the SSH user name for use when establishing tunneling connections with other devices.</text>
ssh username <text>  Sets the SSH user name for use when establishing tunneling connections with other devices.</text>
neling connections with other devices.
tcp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  <milliseconds> = timer value, in milliseconds.</milliseconds></milliseconds>
validate certificate disable  Skips verification of the server certificate when connecting.
validate certificate enable Requires verification of the server certificate when connecting.
vip disable Makes connections using the specified Address.
vip enable Makes connections using the VIP name.
vip name <text> Sets the VIP name.</text>
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> Change to config host level</number>
name <text> Sets the name of the host. <text> = name of the host.</text></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 wh</text>

	distribution
	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 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:15:9) 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 punc-
	tuation:
	123ABC "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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices.

	<text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
validate certificate disable	Skips verification of the server certificate when connect-
	ing.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:14:9) 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></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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no add addispt hos	realisted the confloor turner ALO decrypt Rey.

	D 4 4 14E0 41
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
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></text>	Sets the connect tunnel AES decrypt key with up to 16

ses encrypt key <hexadecimal> ase encrypt key <hexadecimal> ase encrypt key <hexadecimal> ase encrypt key <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. As the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Beach byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Beach byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. Beach byte is represented by a single character. Clears the screen. Clears the screen. Credentials  Clears the screen. Credentials stext&gt; Clears the screen. Beach byte is represented by a single character. Restores the default protocol as "TCP".  default protocol as Restores the default protocol as "TCP".  default trotocol as Restores the default protocol as "TCP".  default protocol to establish tunnel as second connect mode tunnel as second connect tunnel AES decrypt key. Decrease the remote port used to establish tunnel connectons.  Depart the RSA/DSA certificate selection. Removes the remote port used to establish tunnel connectons. Depart the remote port to use for connect mode tunneling.  Protocol top Repeated the protocol for connect mode tunneling.</hexadecimal></hexadecimal></hexadecimal></hexadecimal>		
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*12:2abc Note that quotes must enclose the value if it contains spaces.  Sets the connect funnel AES encrypt key 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  cirsom  Clears the screen.  Credentials <fext> Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  exit  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  no aes decrypt key no aes encrypt key Removes the connect tunnel AES decrypt key. No aes encrypt key Removes the connect tunnel AES encrypt key. No credentials  Clears the SA/DSA certificate selection.  Removes the remote port used to establish tunnel connect tone tunnel AES encrypt key. Removes the remote port used to establish tunnel connect tone to the set of the selection.  Removes the remote port used to establish tunnel connect tone to port used to establish tunnel connect tone to the selection.  Removes the remote port used to establish tunnel connect to top and to use the connect mode tunneling.  Protocol ssh Uses SSH protocol for connect mode tunneling.  Protocol top Uses SSH protocol for connect mode tunneling.  Protocol top Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol top Uses TCP protocol (with IAC) for connect mode tunneling.  Protocol udp Uses UDP protocol (with IAC) for connect mode tunneling.  Protocol udp AES encryption for connect mode tunneling.  Show Show the current configuration.</fext>		Note that quotes must enclose the value if it contains
bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces. auto show statistics  cirsorn  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 top keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connections.  no aes decrypt key  Removes the connect tunnel AES decrypt key.  no credentials  Clears the RSA/DSA certificate selection.  no port  Removes the connect unnel AES encrypt key.  no credentials  Clears the RSA/DSA certificate selection.  no port  Removes the remote port used to establish tunnel connections.  no ssh username  no top keep alive  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  No vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSL protocol for connect mode tunneling.  protocol top  Uses TCP protocol for connect mode tunneling.  protocol top uses TCP protocol (with AES encryption for connect mode tunneling.  protocol dep  protocol dep  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	aes encrypt key <hexadecimal></hexadecimal>	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains
cliscrn  Clears the screen.  credentials <text> Selects the RSA/DSA certificates by name for the SSL client.  default protocol  Restores the default protocol as "TCP".  default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 port  Removes the remote port used to establish tunnel connections.  no ssh username  Removes the remote port used to establish tunnel connections.  no sth username  Removes the remote port used to establish tunnel connections.  so ssh username  Removes the sSH user name.  Disables the connect mode TCP keep alive timeout.  no vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSH protocol for connect mode tunneling.  protocol ssp user scheme to post to use for connect mode tunneling.  Uses TCP 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 tcp uses TCP protocol for connect mode tunneling.  protocol udp  Uses TCP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show uses the current configuration.  Show the current configuration.  Show bistory  CLI session.</text>	aes encrypt key text <text></text>	bytes.  Each byte is represented by a single character.  Note that quotes must enclose the value if it contains
credentials <text>  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  no address  Removes the remote host address used to establish tunneling connect tunnel AES decrypt key.  no aes encrypt key  Removes the connect tunnel AES decrypt key.  no aes encrypt 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 SSH user name.  no top keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  vnumber&gt;  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  protocol ssh  Uses SSL protocol for connect mode tunneling.  protocol top  Uses TCP protocol with AES encryption for connect mode tunneling.  protocol tep aes  Uses UDP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Show  Show she current configuration.  Displays the last 20 commands entered during the current CLI session.</text>	auto show statistics	show connection statistics
default protocol  default trop keep alive  default trop keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  Removes the remote host address used to establish tunneling connections.  Removes the connect tunnel AES decrypt key.  Ro aes encrypt key  Removes the connect tunnel AES encrypt key.  Ro 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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the VIP name.  Disables the connect mode TCP keep alive timeout.  Ro vip name  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roundber> Sets the remote port to use for connect mode tunneling.  rotocol 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 tep aes  Uses TOP protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	clrscrn	Clears the screen.
default tcp keep alive  Restores the default 45 second connect mode TCP keep alive timeout.  Exits to the next higher level.  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 remote port used to establish tunnel connections.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  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 tep aes  Uses TCP protocol with AES encryption for connect mode tunneling.  Protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  Protocol udp  Uses UDP protocol or connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp aes  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.	credentials <text></text>	
exit Exits to the next higher level.  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 port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  no top keep alive Disables the connect mode TCP keep alive timeout.  no vip name Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp Uses UDP protocol (with AES encryption for connect mode tunneling.  protocol udp Shows Bows Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	default protocol	Restores the default protocol as "TCP".
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 RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  roumber> Sets the remote port to use for connect mode tunneling.  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 IAC) for connect mode tunneling.  protocol telnet Uses UDP protocol (with IAC) for connect mode tunneling.  protocol 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.	default tcp keep alive	· ·
neling connections.  no aes decrypt key Removes the connect tunnel AES decrypt key.  no aes encrypt key Removes the connect tunnel AES encrypt key.  Clears the RSA/DSA certificate selection.  no port Removes the remote port used to establish tunnel connections.  no ssh username Removes the SSH user name.  No top keep alive Disables the connect mode TCP keep alive timeout.  No vip name Removes the VIP name Removes the VIP name  Sets the remote port to use for connect mode tunneling. <a href="mailto:rnumber">rnumber</a> Uses SSH protocol for connect mode tunneling.  protocol ssh 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 UDP protocol for connect mode tunneling.  protocol 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.	exit	Exits to the next higher level.
no aes 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.  Removes the VIP name.  Port <number> Sets the remote port to use for connect mode tunneling.  rotocol ssh Uses SSH protocol for connect mode tunneling.  Protocol tcp Uses TCP protocol for connect mode tunneling.  Protocol telnet Uses TCP protocol (with IAC) for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.</number>	no address	
no credentials  Clears the RSA/DSA certificate selection.  Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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 udp  Uses UDP protocol with AES encryption for connect mode tunneling.  protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.	no aes decrypt key	Removes the connect tunnel AES decrypt key.
Removes the remote port used to establish tunnel connections.  Removes the SSH user name.  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Sets the remote port to use for connect mode tunneling.  rotocol 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.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  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.	no aes encrypt key	Removes the connect tunnel AES encrypt key.
nections.  no ssh username  Removes the SSH user name.  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  Sets the remote port to use for connect mode tunneling.  no top keep alive  Uses SSH protocol for connect mode tunneling.  protocol ssh  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  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.</number>	no credentials	Clears the RSA/DSA certificate selection.
no tcp keep alive  Disables the connect mode TCP keep alive timeout.  Removes the VIP name.  Port <number>  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.  Protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  Displays the last 20 commands entered during the current CLI session.</number></number>	no port	
no vip name  Removes the VIP name.  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.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol for connect mode tunneling.  Sets the remote port to use for connect mode tunneling.  Uses SSH protocol for connect mode tunneling.  Uses TCP 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.	no ssh username	Removes the SSH user name.
port <number></number>	no tcp keep alive	Disables the connect mode TCP keep alive timeout.
cnumber> = number of the port to use.   protocol ssh	no vip name	Removes the VIP name.
protocol ssl  Dises SSL protocol for connect mode tunneling.  Dises TCP protocol for connect mode tunneling.  Dises TCP protocol with AES encryption for connect mode tunneling.  Dises TCP protocol with AES encryption for connect mode tunneling.  Dises Telnet protocol (with IAC) for connect mode tunneling.  Dises UDP protocol for connect mode tunneling.  Dises 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.	port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
protocol tcp protocol tcp aes 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.  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.	protocol ssh	Uses SSH 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.  protocol udp  protocol udp aes  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.	protocol ssl	
tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  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.	protocol tcp	Uses TCP protocol for connect mode tunneling.
ing.  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.	protocol tcp aes	
protocol udp aes  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.	protocol telnet	1.
tunneling.  show Shows the current configuration.  show history Displays the last 20 commands entered during the current CLI session.	protocol udp	Uses UDP protocol for connect mode tunneling.
show history  Displays the last 20 commands entered during the current CLI session.	protocol udp aes	
CLI session.	show	Shows the current configuration.
show statistics show connection statistics	show history	
	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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:12:9) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun-

	123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc
add addrypt hay strongadolitidis	bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:
address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
host 9 (tunnel-connect-host:11:9) level commands	Cata the remate heat to establish time allowed in
write	Stores the current configuration in permanent memory.
vip name <text></text>	Sets the VIP name.
vip enable	Makes connections using the VIP name.
vip disable	Makes connections using the specified Address.
validate certificate enable	Requires verification of the server certificate when connecting.
validate certificate disable	Skips verification of the server certificate when connecting.
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.</milliseconds>
ssh username <text></text>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.</text>
show statistics	show connection statistics
show history	Displays the last 20 commands entered during the current CLI session.
show	Shows the current configuration.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol ssh	Uses SSH protocol for connect mode tunneling.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
no vip name	Removes the VIP name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no ssh username	Removes the SSH user name.
no port	Removes the remote port used to establish tunnel connections.
no credentials	Clears the RSA/DSA certificate selection.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no aes decrypt key	Removes the connect tunnel AES decrypt key.

	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep
clrscrn credentials <text> default protocol</text>	show connection statistics  Clears the screen.  Selects the RSA/DSA certificates by name for the SSL client.  Restores the default protocol as "TCP".

	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:9:9) 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
aes encrypt key <hexadecimal></hexadecimal>	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.
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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:8:9) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep
default top keep alive	alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:7:9) 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
ass assign noy should something	bytes.
	Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punc-
	tuation:
	123ABC "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
aes encrypt key text <text></text>	Sets the connect tunnel AES encrypt key with up to 16
des energh key text stext?	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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tun- neling 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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.

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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:6:9) 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.
	op 2000.
auto show statistics	show connection statistics

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	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <number></number>	Sets the remote port to use for connect mode tunneling. <pre><number> = number of the port to use.</number></pre>
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:5:9) level commands	
address <text></text>	Sets the remote host to establish tunneling connections

	with
	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:4:9) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.

host 9 (tunnel-connect-host:3:9) 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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.

tunneling.  protocol telnet  Uses Telnet protocol (with IAC) for connect mode tunneling.  protocol udp  Uses UDP protocol for connect mode tunneling.  Uses UDP protocol with AES encryption for connect mode tunneling.  show  Shows the current configuration.		
ing.  Uses UDP protocol with AES encryption for connect mode tunneling.  Protocol udp aes  Uses UDP protocol with AES encryption for connect mode tunneling.  Show 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.  top keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  willidate certificate disable  Skips verification of the server certificate when connecting.  Validate certificate enable  Requires verification of the server certificate when connecting.  With a server service with a server certificate when connecting.  Wakes connections using the specified Address.  Vip name   **Requires verification of the server certificate when connecting.  Wakes connections using the specified Address.  Vip name   **Requires verification of the server certificate when connecting.  Wakes connections using the VIP name.  **Sets the VIP name.  **Sets the VIP name.  **Stores the current configuration in permanent memory.  **Nost 9 (unnel-connect-host-2:9) level commands  address   **Sets the vip name.  **Sets the connect tunnel AES decrypt key with up 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*** 12.3a.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 **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 encrypt key 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</milliseconds>	protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
Uses UDP protocol with AES encryption for connect mode tunnelling.  show  Shows the current configuration.  Shows the current configuration.  Shows the tourent configuration.  Shows statistics  show connection statistics  show connection statistics  show connection statistics  show connections statistics  show connections with other devices.  step keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  spilliseconds&gt; = 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.  vip disable  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  Stores the current configuration in permanent memory.  host 9 (tunnel-connect-host:2:3) level commands  address <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 9 (tunnel-connect-host:2:3) level commands  address <text>  Sets the connect tunnel AES decrypt key with up to 16 bytes.  aes decrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Bach byte is represented by a single character.  Note that quotes must enclose the value if it contains spaces.  aes encrypt key <hexadecimal>  Sets the connect tunnel AES decrypt key 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' 12,3ABC 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 3ABC' 12 3ABC' 12 3A</hexadecimal></hexadecimal></text></text></milliseconds>	protocol telnet	I.
tunneling.  Shows the current configuration.  Show history  Displays the last 20 commands entered during the current CLI session.  Show statistics  Show connection statistics  Sats the SSH user name for use when establishing tunneling connections with other devices.	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.  It devices a SSH user name for use when establishing tunneling connections with other devices.  It devices a SSH user name.  It cp keep alive <milliseconds>  Enables TCP keep alive for connect mode tunneling and sets the timer.  It is a still seconds a still seconds and sets the 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.  Vip disable  Makes connections using the specified Address.  Vip enable  Makes connections using the VIP name.  Vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 3 (tunnel-connect-host:2:9) level commands  address <text>  Sets the remote host to establish tunneling connections with.  It 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 encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex 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  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 12.3a.bc 12.3a.bc  Note that quotes must enclose the value if it contains spaces.</text></text></milliseconds>	protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
CLI session.	show	Shows the current configuration.
Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.   tcp keep alive <milliseconds> Enables TCP keep alive for connect mode tunneling 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.   vip disable Makes connections using the specified Address.   vip enable Makes connections using the VIP name.   vip name <text> Sets the VIP name.   write Stores the current configuration in permanent memory.   host 9 (tunnel-connect-host:2:9) level commands   address <text> Sets the remote host to establish tunneling connections with.   <text> = IP address or host name of the remote host.   aes decrypt key <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. Sets the connect tunnel AES decrypt key 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> Sets the connect tunnel AES encrypt key with up to 16 bytes.   Each byte is represented by two adjacent hex digits.   Bytes may run together or be separated by optional punctuation: 123ABC *12.3A.BC *12.3A.</hexadecimal></hexadecimal></text></text></text></milliseconds></milliseconds></text>	show history	Displays the last 20 commands entered during the current CLI session.
neling connections with other devices.	show statistics	show connection statistics
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.  vip disable  Makes connections using the specified Address.  vip enable  vip name <text>  Sets the VIP name.  vith name.  vith name.  Sets the VIP name.  Sets the current configuration in permanent memory.  host 9 (tunnel-connect-host:2:9) level commands  address <text>  Sets the remote host to establish tunneling connections with.  **\text&gt; = 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.  aes encrypt key <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 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 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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</hexadecimal></text></text>	ssh username <text></text>	neling connections with other devices.
ing.     requires verification of the server certificate when connecting.     Requires verification of the server certificate when connecting.     Vip disable	tcp keep alive <milliseconds></milliseconds>	sets the timer.
necting.  vip disable  Makes connections using the specified Address.  vip enable  Makes connections using the VIP name.  vip name <text>  Sets the VIP name.  Stores the current configuration in permanent memory.  host 9 (tunnel-connect-host:2:9) 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 optional punctuation:  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text></text></text>	validate certificate disable	I. ·
vip enable  vip name <text> Sets the VIP name.  Sets the VIP name.  Sets the VIP name.  Stores the current configuration in permanent memory.  Nost 9 (tunnel-connect-host:2:9) 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 optional punctuation:  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.</text></text></text>	validate certificate enable	
vip name <text> Sets the VIP name.  Stores the current configuration in permanent memory.  host 9 (tunnel-connect-host:2:9) 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.  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.  Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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 two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 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.</text></text></text></text></text>	vip disable	Makes connections using the specified Address.
write    Stores the current configuration in permanent memory.   Stores the current current configuration in permanent memory.   Stores the current current current memory in the following memory in	vip enable	Makes connections using the VIP name.
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 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.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	vip name <text></text>	Sets the VIP name.
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 optional punctuation:  123ABC "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 &lt; text&gt;  Sets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  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.</text>		
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 23ABC "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.</text></text>	write	Stores the current configuration in permanent memory.
aes decrypt key <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.  3ets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  3ets the connect tunnel AES encrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  3ets the connect tunnel AES encrypt key with up to 16 bytes.  Sets the connect tunnel AES encrypt key with up to 16 bytes.  3ets the connect tunnel AES encrypt key with up to 16 bytes.</hexadecimal>	- 12	Stores the current configuration in permanent memory.
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.  3 Sets the connect tunnel AES encrypt key with up to 16 bytes.  5 Sets the connect tunnel AES encrypt key with up to 16 bytes.  5 Sets the connect tunnel AES encrypt key with up to 16 bytes.	host 9 (tunnel-connect-host:2:9) level commands	Sets the remote host to establish tunneling connections with.
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.  aes encrypt key text <text> Sets the connect tunnel AES encrypt key with up to 16 bytes.</text>	host 9 (tunnel-connect-host:2:9) 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>
bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "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.</text>	host 9 (tunnel-connect-host:2:9) level commands address <text></text>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.  Sets the connect tunnel AES decrypt key with up to 16 bytes.  Each byte is represented by two adjacent hex digits.  Bytes may run together or be separated by optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>
bytes.	host 9 (tunnel-connect-host:2:9) level commands address <text> aes decrypt key <hexadecimal></hexadecimal></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</text>
	host 9 (tunnel-connect-host:2:9) level commands address <text>  aes decrypt key <hexadecimal>  aes decrypt key text <text></text></hexadecimal></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 optional punctuation:  123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc  Note that quotes must enclose the value if it contains</text>

	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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
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.
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 tun- neling connections with other devices. <text> = SSH user name.</text>
tcp keep alive <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <text></text>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:1:9) 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 <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 tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
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 port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port < <i>number</i> >	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.</number>

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.
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 <milliseconds></milliseconds>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer 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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <text></text>	Sets the VIP name.
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 < <i>number</i> >	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.
http (config-http) level commands	
auth <uri></uri>	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. <ur> <ur> <ur> <uri><uri><uri><uri><uri><uri><uri><uri< td=""></uri<></uri></uri></uri></uri></uri></uri></uri></ur></ur></ur>
auth type <uri> ssl</uri>	Sets the authentication type for an HTTP server authentication directive to SSL. <ur> <ur> <ur> <ur> <uri> = URI of the server.</uri></ur></ur></ur></ur>
auth type <uri> ssl-basic</uri>	Sets the authentication type for an HTTP server authentication directive to SSL-Basic. <ur><ur><uri><uri><uri><uri><uri><uri><uri><uri< td=""></uri<></uri></uri></uri></uri></uri></uri></uri></ur></ur>
auth type <uri> ssl-digest</uri>	Sets the authentication type for an HTTP server authentication directive to SSL-Digest. <ur> <ur> <li>- URI of the server.</li> </ur></ur>
authentication timeout <minutes></minutes>	For any Digest AuthType, sets the timeout for authentication. <pre><minutes> = authentication timeout value.</minutes></pre>
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.
default secure protocols	Restores the default secure protocol selections.
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 <number></number>	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.
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.
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.
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 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.
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.
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.
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.
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.
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.
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.
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.
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.
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 protocol	Restores the default protocol on the line.
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 <li>line&gt;</li>	Enters the line level. <pre><li><li>&lt; = number of the line (serial port) to be configured.</li></li></pre>

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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
threshold threshold /bytes>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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> >  line 10 (line:10) level commands	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>

baud rate baud rate bits per second> Sets the line speed. bits per second> Set the speed second> Standard speeds include 1200, 2400, 4800, 9600, 19200, and 50 on.  Glear line counters Sets the serial counters to zero.  Clears the screen.  Clears the screen.  Clears the screen.  Clears the screen.  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  Enables user to enter a custom string at boot time to enter command mode.  Command mode serial string  Sets a string that can be entered at boot time to enter command mode.  Sets a string = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <a href="mailtiseconds">mailtiseconds</a> Sets boot-up wait time for command mode.  **String= text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <a href="mailtiseconds">mailtiseconds</a> Sets boot-up wait time for command mode serial string.  Configures line with the current value of settings.  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  default baud rate  default baud rate  default baud rate  default speed of 9600 bits per second.  Restores the default of eight data bits.  Restores the default of one stop bit.  default thory control  Restores the default of one stop bit.  default stop bits  Restores the default of one stop bit.  Restores the default to posity.  Restores the default to	auto show statistics	Continuously displays line statistics.
clear line counters  closure  Clears the screen.  Clears the screen.  Clears the screen.  Clears the screen.  Sets the current line to always be in command mode.  command mode echo serial string disable  Command mode echo serial string enable  Command mode echo serial string enable  Command mode serial string  Command mode.  Command mode serial string  Command mode.  Command mode serial string  Command mode.  Command mode serial string <a href="#serial-pot-time-to-enter-command-mode">Sets a string that can be entered at boot time to enter command mode.  Command mode serial string <a href="#serial-pot-time-to-enter-command-mode">Sets a string that can be entered at boot time to enter command mode.  Command mode signon message <a href="#serial-pot-time-to-enter-command-mode">Sets a string that can be entered at boot time to enter command mode.  Command mode signon message <a href="#serial-pot-time-to-enter-command-mode">Sets a string that can be entered at boot time to enter command mode.  Command mode signon message <a #serial-string-serial<="" href="#serial-pot-time-to-enter-command-mode-command-mode-command-mode-command-mode-command-com-&lt;/td&gt;&lt;td&gt;baud rate &lt;br/&gt;bits per second&gt;&lt;/td&gt;&lt;td&gt;Sets the line speed. &lt;br/&gt; &lt;br&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;cirsom  Clears the screen.  Clears the screen.  Command mode always  Sets the current line to always be in command mode.  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-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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is no command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string.  Configure current settings  Configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  default baud rate  default baud rate  default baud rate  default baud rate  default data bits  Restores the default of no flow control.  default flow control  Restores the default of no flow control.  default protocol  Restores the default of no parity.  default protocol  Restores the default on the line.  default top bits  Restores the default won character on this line.  default two char  Restores the default tone hardware on this line.  Will can be control on the line.  Does not provide flow control on the line.  Uses shardware (RTS/CTS) flow control on the line.  Uses shardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses shardware (xon/xoff characters) flow control on the line.  Sets to the enable level  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xof&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;command mode always  Command mode echo serial string disable  Command mode echo serial string disable  Command mode echo serial string enable  Command mode serial string enable  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 serial string  Enables user to enter a custom string at boot time to enter command mode.  Command mode serial string &lt;a href=" td=""><td>clear line counters</td><td>Sets the serial counters to zero.</td></a></a></a></a></a>	clear line counters	Sets the serial counters to zero.
command mode echo serial string disable  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   Enables user to enter a custom 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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode string.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode.  **String>= text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  W	clrscrn	Clears the screen.
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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets as sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets as sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string.  comfigure current settings  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  default baud rate  default baud rate  Restores the default speed of 9600 bits per second.  default data bits  Restores the default of no parity.  default flow control  default parity  Restores the default of no parity.  default protocol  Restores the default of no parity.  Restores the default of no parity.  Restores the default for posity.  Restores the default to for both bits.  Restores the default for both	command mode always	Sets the current line to always be in command mode.
the CLI.  Command mode serial string  Enables user to enter a custom string at boot time to enter command mode.  Command mode serial string <a href="string">string</a> Sets a string that can be entered at boot time to enter command mode.	command mode echo serial string disable	
command mode serial string <string>  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  setring&gt; = text with possible binary characters. Within {} use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay. command mode signon message <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. command mode wait time <milliseconds> Sets boot-up wait time for command mode serial string. <milliseconds> = wait time. configure current settings Configures line with the current value of settings. data bits 7 Uses seven bits for data on the line. default baud rate default baud rate default baud rate default data bits Restores the default of eight data bits. default data bits Restores the default of no flow control. default parity Restores the default of no flow control. default parity Restores the default of no parity. default stop bits Restores the default protocol on the line. default stop bits Restores the default woff character on this line. Restores the default woff character on this line. default work char Restores the default woff character on this line. Exits to the enable level Uses hardware (RTS/CTS) flow control on the line. flow control hardware flow control software Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) 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. Flow control software Line <inv td="" wil<="" will=""  =""><td>command mode echo serial string enable</td><td></td></inv></milliseconds></milliseconds></string></string></string>	command mode echo serial string enable	
command mode.   command mode.	command mode serial string	
when the device boots and when the line is in command mode.	command mode serial string <string></string>	command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
<milliseconds> = wait time. 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 protocol Restores the default protocol on the line. default stop bits Restores the default of one stop bit. Restores the default of one stop bit. Restores the default worf character on this line. default xoff char default xoff char Restores the default xoff character on this line. default xon char Restores the default xon character on this line. Exits to the enable level Uses hardware (RTS/CTS) flow control on the line. flow control hardware Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) flow control on the line. 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 Enters the line level. sline&gt; = number of the line (serial port) to be configured.</milliseconds>	command mode signon message <string></string>	when the device boots and when the line is in command mode. <string> = text with possible binary characters.</string>
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 protocol  Restores the default protocol on the line.  default stop bits  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default worst of char one stop bit.  Restores the default worst of character on this line.  default xon char  Restores the default xon character on this line.  Exits to the enable level  flow control hardware  Uses hardware (RTS/CTS) flow control on the line.  flow control software  Uses software (xon/xoff characters) flow control on the line.  gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills session  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li><li></li></li></li></li></li></li></milliseconds>	command mode wait time <milliseconds></milliseconds>	
data bits 8  default baud rate  default baud rate  default baud rate  Restores the default speed of 9600 bits per second.  Restores the default of eight data bits.  default flow control  Restores the default of no flow control.  Restores the default of no parity.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of noe stop bit.  Restores the default wof one stop bit.  Restores the default wof one stop bit.  Restores the default woff character on this line.  Restores the default woff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  flow control hardware  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li><li><li></li></li></li></li></li></li></li></milliseconds>	configure current settings	Configures line with the current value of settings.
default baud rate  default data bits  default flow control  default parity  default protocol  default stop bits  Restores the default of no parity.  default threshold  default work char  default xoff char  default xoff char  default work control  default xoff char  default xor char  exit  Exits to the enable level  flow control none  flow control software  gap timer <milliseconds>  Kills command mode session on the Line  Restores the default speed of 9600 bits per second.  Restores the default of no flow control to be configured.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default to no estop bit.  Restores the default xoff character on this line.  Uses the default xoff character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <incenter <incenter="" level.="" level.<="" line="" td="" the=""><td>data bits 7</td><td>Uses seven bits for data on the line.</td></incenter></milliseconds>	data bits 7	Uses seven bits for data on the line.
default data bits  default flow control  Restores the default of no flow control.  Restores the default of no parity.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  flow control hardware  Uses hardware (RTS/CTS) flow control on the line.  flow control software  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li>	data bits 8	Uses eight bits for data on the line.
default flow control  default parity  default protocol  default stop bits  default threshold  default xoff char  default xon char  exit  flow control hardware  flow control none  flow control software  gap timer < milliseconds>  Kills command mode session on the Line  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <incere be="" configured.<="" control="" td="" to=""><td>default baud rate</td><td>Restores the default speed of 9600 bits per second.</td></incere>	default baud rate	Restores the default speed of 9600 bits per second.
default parity  default protocol  Restores the default protocol on the line.  default stop bits  Restores the default of one stop bit.  default threshold  Restores the default threshold.  Restores the default xoff character on this line.  default xoff char  Restores the default xoff character on this line.  default xon char  Restores the default xon character on this line.  Exits to the enable level  flow control hardware  Uses hardware (RTS/CTS) flow control on the line.  flow control software  Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <li>line&gt; = number of the line (serial port) to be configured.</li></milliseconds>	default data bits	Restores the default of eight data bits.
default protocol  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  I Uses hardware (RTS/CTS) flow control on the line.  I Uses not provide flow control on the line.  I Uses software (xon/xoff characters) flow control on the line.  Gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Inters the line level.  I chiers the line level.  I chiers the line (serial port) to be configured.</milliseconds>	default flow control	Restores the default of no flow control.
default stop bits  default threshold  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Sexits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  Inters the line (serial port) to be configured.	default parity	Restores the default of no parity.
default threshold  default xoff char  default xoff char  default xoff char  default xon char  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li>	default protocol	Restores the default protocol on the line.
default xoff char  default xon char  default xon char  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <li><li><li><li>&lt; = number of the line (serial port) to be configured.</li></li></li></li>	default stop bits	Restores the default of one stop bit.
default xon char exit  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <incere <incere="" control="" enters="" level.="" line="" line.="" line.<="" on="" td="" the=""><td>default threshold</td><td>Restores the factory default threshold.</td></incere>	default threshold	Restores the factory default threshold.
Exits to the enable level  flow control hardware  flow control none  flow control software  flow control software  gap timer <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  Enters the line level.  <li><li><li><e (xon="" <="" after="" be="" been="" character.="" characters)="" command="" control="" data="" enters="" flow="" forwarded="" gap="" has="" if="" in="" it="" kills="" last="" level.="" line="" line.="" milliseconds.="" mode="" not="" on="" provide="" received,="" session="" sets="" since="" software="" some="" td="" the="" this="" time="" timer="" uses="" will="" xoff=""></e></li></li></li></milliseconds>	default xoff char	Restores the default xoff character on this line.
flow control hardware  flow control none  flow control software  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <li><li><li><li>&lt; = number of the line (serial port) to be configured.</li></li></li></li>	default xon char	Restores the default xon character on this line.
flow control none  flow control software  flow control software  Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <li><li><li>&lt;= number of the line (serial port) to be configured.</li></li></li></milliseconds>	exit	Exits to the enable level
flow control software  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <li><li>&lt; line&gt; = number of the line (serial port) to be configured.</li></li>	flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
gap timer <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  Enters the line level.  <li><li><li>= number of the line (serial port) to be configured.</li></li></li></milliseconds>	flow control none	Does not provide flow control on the line.
received, it will be forwarded after this time since the last character.  kill session  Kills command mode session on the Line  line < line>  Enters the line level. < line> = number of the line (serial port) to be configured.	flow control software	'
line  Enters the line level. <li>&lt; line&gt; = number of the line (serial port) to be configured.</li>	gap timer <milliseconds></milliseconds>	received, it will
<pre><li>&lt; = number of the line (serial port) to be configured.</li></pre>	kill session	Kills command mode session on the Line
name <text> Sets the name for this line.</text>	line <li>line&gt;</li>	
	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. <pre><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></pre>
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 <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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.

	I
baud rate bits per second>	Sets the line speed.   <br< td=""></br<>
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
Command mode echo serial sumg disable	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 protocol	Restores the default protocol on the line.
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 <li>line&gt;</li>	Enters the line level. <pre><li><li>&lt;= number of the line (serial port) to be configured.</li></li></pre>
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. <li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li>
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. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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 12 (line:12) 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, nd so on.
ets the serial counters to zero.
Clears the screen.
ets the current line to always be in command mode.
Disables user-defined serial boot string to be echoed in the CLI.
nables user-defined serial boot string to be echoed in ne CLI.
nables user to enter a custom string at boot time to enter ommand mode.
tets a string that can be entered at boot time to enter ommand mode. string> = text with possible binary characters. Vithin [] use binary decimal up to 255 or hex up to 0xFF. Vithin {} specify decimal milliseconds time delay.
tets a sign-on message that is sent from the serial port when the evice boots and when the line is in command mode. string> = text with possible binary characters.  Vithin [] use binary decimal up to 255 or hex up to 0xFF.
ets boot-up wait time for command mode serial string. milliseconds> = wait time.
Configures line with the current value of settings.
Ises seven bits for data on the line.
Ises eight bits for data on the line.
testores the default speed of 9600 bits per second.
lestores the default of eight data bits.
lestores the default of no flow control.
lestores the default of no parity.
testores the default protocol on the line.
lestores the default of one stop bit.
lestores the factory default threshold.
lestores the default xoff character on this line.
testores the default xon character on this line.
xits to the enable level
Ises hardware (RTS/CTS) flow control on the line.
oes not provide flow control on the line.
lses software (xon/xoff characters) flow control on the ne.
ets the gap timer in milliseconds. If some data has been eceived, it will e forwarded after this time since the last character.
ills command mode session on the Line
inters the line level. line> = number of the line (serial port) to be configured.
ets the name for this line.
testores the serial counters to the aggregate values.
bisables 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. <li>line&gt; = number of the terminal line (serial port) to be configured.</li>
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. <li><li><li>= number of the tunnel line (serial port) to be configured.</li></li></li>
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.          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 protocol	Restores the default protocol on the line.
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. <li><li><li>&lt; = number of the line (serial port) to be configured.</li></li></li>
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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
threshold <td>Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.</td>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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.    

Clears the screen.  Clears the screen.  Command mode always  Sets the current line to always be in command mode.  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-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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Settings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  Configures line with the current value of settings.  Configures the default of eight data on the line.  Configures the default of no flow control.  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Configures the default for hor parity.  Restores the default of no hor parity.  Restores the default of no hor parity.  Restores the default of hor parity.  Re</milliseconds>		Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
Sets the current line to always be in command mode.  command mode echo serial string disable the CLI.  Command mode echo serial string enable Enables user-defined serial boot string to be echoed in the CLI.  Command mode 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>  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.  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.  Command mode wait time <*milliseconds> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <*milliseconds> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <*milliseconds> = wait time.  **Sets boot-up wait time for command mode serial string.**  **milliseconds> = wait time.  **Configures line with the current value of settings.  data bits 7	clear line counters	Sets the serial counters to zero.
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.  Sets a string that can be entered at boot time to enter command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] so binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets a sign-on message that is sent from the serial port when the line is in command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets as sign-on message that is sent from the serial port when the device boots and when the line is in command mode existings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode serial string serial port when the line serial</milliseconds>	clrscrn	Clears the screen.
the CLI.  Command mode echo serial string enable  Enables user to enter a custom 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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string.  Configure current settings  Configure current settings  Configures line with the current value of settings.  Uses seven bits for data on the line.  Uses seven bits for data on the line.  Uses seven bits for data on the line.  Restores the default speed of 9600 bits per second.  default baud rate  Restores the default of eight data bits.  default flow control  Restores the default of no flow control.  Restores the default for no flow control.  Restores the default protocol on the line.  default protocol  Restores the default of no parity.  default protocol  Restores the default of one stop bit.  Restores the default vor character on this line.  default two char  Restores the default vor character on this line.  Exit to the enable level  Sexit to the enable level  Uses software (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (RTS/CTS) flow control on the line.  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  Kill session  Lines = Innumber of the line (serial port) to be configured.	command mode always	Sets the current line to always be in command mode.
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.  Sets a string that can be entered at boot time to enter command mode.  Strings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] specify decimal impliesconds time delay.  Command mode signon message <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.  Strings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Dommand mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  Configure current settings  Configures line with the current value of settings.  Duses seven bits for data on the line.  Uses seven bits for data on the line.  Uses seight bits for data on the line.  Default bauf rate  Restores the default speed of 9600 bits per second.  Restores the default of eight data bits.  Restores the default of no parity.  Default parity  Restores the default of no parity.  Default parity  Restores the default of no parity.  Default protocol  Restores the default of no parity.  Default protocol  Restores the default of no parity.  Default protocol  Restores the default to fone stop bit.  Restores the default of none stop bit.  Restores the default son character on this line.  Restores the default son chara</milliseconds></string>	command mode echo serial string disable	
command mode.  Sets a string that can be entered 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 {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal my to 0xFF. Within {} s	command mode echo serial string enable	
command mode. <asting> text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within [] use binary decimal up to 255 or hex up to 0xFF. Within [] specify decimal milliseconds time delay. Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <a trimp=""> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.   command mode wait time <milliseconds> Sets boot-up wait time for command mode serial string. <a href="mailto:cmilliseconds">cmilliseconds&gt;</a> = wait time.   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 seyen bits for data on the line.    default baud rate Restores the default speed of 9600 bits per second.    default flow control Restores the default of no flow control.    default parity Restores the default of no parity.    default protocol Restores the default of no parity.    default protocol Restores the default protocol on the line.    default stop bits Restores the default protocol on the line.    default threshold Restores the default wor character on this line.    default wor char Restores the default wor character on this line.    default wor char Restores the default wor character on the line.    liow control hardware Uses hardware (RTS/CTS) flow control on the line.    flow control hardware Uses software (xon/xoff characters) flow control on the line.    liow control software Sets the gap timer in millise</milliseconds></a></asting>	command mode serial string	, , , , , , , , , , , , , , , , , , ,
when the device boots and when the line is in command mode. <pre></pre>	command mode serial string <string></string>	command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
<milliseconds> = wait time. 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 protocol Restores the default protocol on the line. default stop bits Restores the default of one stop bit. Restores the default of one stop bit. Restores the default wof character on this line. default woff char default woff character on this line. default xon char Restores the default xon character on this line. default xon char Restores the default xon 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. Does not provide flow control on the line. Glow control software Uses software (xon/xoff characters) flow control on the line. Gets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character. Kills command mode session on the Line Enters the line level. Inex = number of the line (serial port) to be configured. Sets the name for this line.</milliseconds>	command mode signon message <string></string>	when the device boots and when the line is in command mode. <string> = text with possible binary characters.</string>
data bits 7  data bits 8  default baud rate  default baud rate  default data bits  default flow control  default protocol  default treshold  default word char  default stop bits  default word char  default word character on this line.  default word character on this line.  Exits to the enable level  down control hardware  flow control none  Does not provide flow control on the line.  duses software (xon/xoff characters) flow control on the line.  default will  be forwarded after this time since the last character.  kill session  kills command mode session on the Line  Enters the line level. <input cline="" series=""/> = number of the line (serial port) to be configured.	command mode wait time <milliseconds></milliseconds>	
data bits 8  Uses eight bits for data on the line.  default baud rate  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 no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of none stop bit.  Restores the default of none stop bit.  Restores the default woff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  flow control hardware  Uses hardware (RTS/CTS) flow control on the line.  flow control software  Uses software (xon/xoff characters) flow control on the line.  Gap time <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li></li><li><li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li>&lt;</li></li></li></li></li></li></milliseconds>	configure current settings	Configures line with the current value of settings.
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 flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default was default threshold.  Restores the default was character on this line.  Exits to the enable level  Flow control hardware  Row control hardware  Row control none  Does not provide flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inne> enters the line (serial port) to be configured.</inne>	data bits 7	Uses seven bits for data on the line.
default data bits  default flow control  default parity  default protocol  default stop bits  default work control  default work control  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default threshold.  Restores the default work control default threshold.  Restores the default work character on this line.  Exits to the enable level  flow control hardware  flow control hardware  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <iner> = number of the line (serial port) to be configured.  Sets the name for this line.</iner></milliseconds>	data bits 8	Uses eight bits for data on the line.
default flow control  default parity  default protocol  default protocol  default stop bits  default treshold  default word char  default word character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <inne> = number of the line (serial port) to be configured.  Sets the name for this line.</inne>	default baud rate	Restores the default speed of 9600 bits per second.
default parity  default protocol  default stop bits  default threshold  default xoff char  default xon char  exit  flow control none  flow control software  flow control software  gap timer <milliseconds>  Sets the gap timer in milliseconds.  Kills command mode session on the Line  Enters the line (serial port) to be configured.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <inex -="" -<="" exit="" td=""><td>default data bits</td><td>Restores the default of eight data bits.</td></inex></milliseconds>	default data bits	Restores the default of eight data bits.
default protocol  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default von character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inne>  Enters the line (serial port) to be configured.  Sets the name for this line.</inne>	default flow control	Restores the default of no flow control.
Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solve control hardware  Uses hardware (RTS/CTS) flow control on the line.  Solve control software  Uses software (xon/xoff characters) flow control on the line.  Solve control software  Uses software (xon/xoff characters) flow control on the line.  Solve 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  Enters the line level. <inne> enumber of the line (serial port) to be configured.  Sets the name for this line.</inne>	default parity	Restores the default of no parity.
default threshold  default xoff char  default xoff char  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Illuses hardware (RTS/CTS) flow control on the line.  Illuses software (xon/xoff characters) flow control on the line.  Illuses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inner <="" li="">Inner &lt; line &gt; = number of the line (serial port) to be configured.  Sets the name for this line.</inner>	default protocol	Restores the default protocol on the line.
Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <incenter (serial="" be="" configured.="" for="" line="" line.<="" name="" of="" port)="" sets="" td="" the="" this="" to=""><td>default stop bits</td><td>Restores the default of one stop bit.</td></incenter>	default stop bits	Restores the default of one stop bit.
Restores the default xon character on this line.  Exit Exits to the enable level  Glow control hardware  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li>	default threshold	Restores the factory default threshold.
Exits to the enable level  flow control hardware  flow control none  flow control none  flow control software  flow control software  gap timer <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  Enters the line level.  <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li></milliseconds>	default xoff char	Restores the default xoff character on this line.
flow control hardware  flow control none  flow control none  flow control software  flow control software  Grow control software  flow control software  Grow control software  Grow control software  Grow control software  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  Inner < text>  Sets the name for this line.	default xon char	Restores the default xon character on this line.
flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.</li></li></li></li></milliseconds>	exit	Exits to the enable level
I Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.</li></li></li></li></milliseconds>	flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
line.   gap timer <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 &lt; line &gt;</milliseconds>	flow control none	Does not provide flow control on the line.
received, it will be forwarded after this time since the last character.  kill session  Kills command mode session on the Line  Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.</li>	flow control software	1
line <li>line &gt; Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.</li></li>	gap timer <milliseconds></milliseconds>	received, it will
<pre><li><li>&lt; = number of the line (serial port) to be configured.</li></li></pre> name <text> Sets the name for this line.</text>	kill session	Kills command mode session on the Line
	line <line></line>	
no clear line counters Restores the serial counters to the aggregate values.	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	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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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 15 (line:15) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed.   <br< td=""></br<>

	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 protocol	Restores the default protocol on the line.
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. <li><li>&lt;= number of the line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the terminal line (serial port) to be configured.</li></li>
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. <li><li>&lt; = number of the tunnel line (serial port) to be configured.</li></li>
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.    dits per 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 no parity.
default protocol	Restores the default protocol on the line.
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. <li>&lt;= number of the line (serial port) to be configured.</li>
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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
threshold threshold threshold threshold 	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <line></line>	Enters the tunnel level. <pre><li><li><li>= number of the tunnel line (serial port) to be configured.</li></li></li></pre>
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 2 (line:2) 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 protocol	Restores the default protocol on the line.
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the terminal line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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 3 (line:3) level commands	
auto show statistics	Continuously displays line statistics.
baud rate bits per second>	Sets the line speed.         Sets the line speed.

Clears the screen.  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  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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Setting = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets be set up to a set up to 0xFF.  Sets boot-up wait time for command mode serial string.  Sets be set with possible binary characters.  Sets be default and the current value of settings.  Sets be factory to default of no flow control.  Restores the default on the line.  Sets be factory de</milliseconds>		Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
Sets the current line to always be in command mode.  command mode echo serial string disable  command mode echo serial string enable  Enables 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 defined serial boot string to be echoed in the CLI.  Enables 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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode signon message string.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Enables user-to what time for command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode serial string.  Sets boot-up wait time for data on the line.  Uses seven bits for data on the line.  Sets seven bits for data on the line.  Sets the default for no flow control.  Restores the default of no parity.  Restores the default of no parity.  Restores the default p	clear line counters	Sets the serial counters to zero.
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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Settings = text with possible binary characters.  Within    use binary decimal up to 255 or hex up to 0xFF.  Within    use binary decimal up to 255 or hex up to 0xFF.  Within    use binary decimal up to 255 or hex up to 0xFF.  Within    use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Individual time command mode seria	clrscrn	Clears the screen.
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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets to sign-on message that is sent from the serial port when the line is in command mode.  Sets boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 25	command mode always	Sets the current line to always be in command mode.
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.  strings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  sstrings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  millisecondss – wait time.  configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  default baud rate  default data bits  Restores the default speed of 9600 bits per second.  default flow control  Restores the default of eight data bits.  default flow control  Restores the default of no flow control.  Restores the default for no flow control.  Restores the default protocol on the line.  default stop bits  Restores the default of no parity.  default protocol  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop b	command mode echo serial string disable	
command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string = text with possible binary characters. Within {} specify decimal milliseconds time delay.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  sating = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. will seconds = wait time.  Configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven 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.  Restores the default of no parity.  default parity  Restores the default of no parity.  default protocol  Restores the default for no parity.  default threshold  Restores the default for no stop bit.  Restores the default tone stop bit.  Restores the default speed on the line.  default wor char  Restores the default wor character on this line.  Restores the default wor character on this line.  Exits to the enable level  liow control hardware  Uses nardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  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  Enters the line level.  eline < line > line > line = line > line = line > line = line > l	command mode echo serial string enable	
command mode.  saftring> = lext with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] specify decimal milliseconds time delay.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  saftring> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven 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 parity  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default for one stop bit.  Restores the default for control one the line.  default threshold  Restores the default for control on the line.  default two character on this line.  Desire the default worf character on this line.  Desire the default worf character on this line.  Desire the default worf character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Does not provide flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff character) flow control on the line.  Does not provide flow control on the line.  Does not provide flow control on the line.  Does not provide flow control on the line.  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 c	command mode serial string	_
when the device boots and when the line is in command mode. <ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr< tr=""><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr< tr=""><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr< tr=""><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr< tr=""><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><ttr><td< td=""><td>command mode serial string <string></string></td><td>command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string></td></td<></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr<></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr<></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr<></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr<></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr></ttr>	command mode serial string <string></string>	command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
<milliseconds> = wait time. 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 seight 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 protocol Restores the default protocol on the line. default threshold Restores the default protocol on the stop bit. Restores the default of one stop bit. Restores the default worf character on this line. default xoff char Restores the default xoff character on this line. default xon char Restores the default xon character on this line. Exits to the enable level Illow control hardware Uses hardware (RTS/CTS) flow control on the line. Illow control none Does not provide flow control on the line. Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) flow control on the line. 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 Enters the line level. Aline&gt; = number of the line (serial port) to be configured. Name &lt; text&gt; Sets the name for this line. Restores the serial counters to the aggregate values.</milliseconds>	command mode signon message <string></string>	when the device boots and when the line is in command mode. <string> = text with possible binary characters.</string>
data bits 7  Uses seven bits for data on the line.  data bits 8  Uses eight bits for data on the line.  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 protocol on the line.  Restores the default of no stop bit.  Restores the default for one stop bit.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.    Ine> = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.	command mode wait time <milliseconds></milliseconds>	
data bits 8  Uses eight bits for data on the line.  default baud rate  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 no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of none stop bit.  Restores the default of none stop bit.  Restores the default woff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Source on the line.  Source of the wontrol none on the line.  Source on the line in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In eximple of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	configure current settings	Configures line with the current value of settings.
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 protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default was off character on this line.  Restores the default xoff character on this line.  Restores the default xor character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Restores the default con character on this line.  Lexits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inne> Enters the line level.  <inne> = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.</inne></inne>	data bits 7	Uses seven bits for data on the line.
Restores the default of eight data bits.  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Exits to the enable level  I Uses hardware (RTS/CTS) flow control on the line.  Row control none  Does not provide flow control on the line.  Does not provide flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  I ine > = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.	data bits 8	Uses eight bits for data on the line.
default flow control  default parity  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default control control control line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the gap timer (anilose control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In extended after this line (serial port) to be configured.  Restores the serial counters to the aggregate values.	default baud rate	Restores the default speed of 9600 bits per second.
Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Restores the default xon character on this line.  Exits to the enable level  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inne>  Enters the line level.  <ine>  Inne &lt; line&gt;  Restores the serial counters to the aggregate values.</ine></inne>	default data bits	Restores the default of eight data bits.
Restores the default protocol on the line.  default stop bits  Restores the default of one stop bit.  Restores the default threshold.  Restores the default xoff char default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <ine> <ine< <ine=""> <ine> <ine> <ine> <ine> <ine> <ine> <ine> <ine> <ine> <i< td=""><td>default flow control</td><td>Restores the default of no flow control.</td></i<></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine<></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine>	default flow control	Restores the default of no flow control.
Restores the default of one stop bit.  Restores the factory default threshold.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Blow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  Inne < line>  Enters the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default parity	Restores the default of no parity.
Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solution (RTS/CTS) flow control on the line.  Solution control none  Does not provide flow control on the line.  Solution control software  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control solution control solution control on the line.  Solution control solution control solution control on the line.  Solution control solution control solution control on the line.  Solution control solution control on the line.  Solution control solution control on th	default protocol	Restores the default protocol on the line.
Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solution control hardware  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Solution control software  Solution control software  Solution control software  Uses software (xon/xoff characters) flow control on the line.  Solution control software in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline < line > = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default stop bits	Restores the default of one stop bit.
Restores the default xon character on this line.  Exit Exits to the enable level  flow control hardware  flow control none  flow control software  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li><li><li><li></li><li><li><li><li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li>&lt;</li></li></li></li></li></li></li></li></li></li></li></li></milliseconds>	default threshold	Restores the factory default threshold.
Exits to the enable level  Glow control hardware  Glow control none  Glow control software  Glow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline > In cline sounters  Glow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline > In cline serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default xoff char	Restores the default xoff character on this line.
flow control hardware  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li>&lt;= number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li></milliseconds>	default xon char	Restores the default xon character on this line.
Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li></li></li></li>	exit	Exits to the enable level
Illuses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li>&lt; = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li>	flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
line.     gap timer <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 <li>line <li>line &gt;   Enters the line level.     <li>  <li>  &lt;   enters the line (serial port) to be configured.     Sets the name for this line.     Restores the serial counters to the aggregate values.  </li></li></li></li></milliseconds>	flow control none	Does not provide flow control on the line.
received, it will be forwarded after this time since the last character.  kill session  Kills command mode session on the Line  Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li>	flow control software	1
Enters the line level. <ine> = number of the line (serial port) to be configured.  name <text> Sets the name for this line.  Restores the serial counters to the aggregate values.</text></ine>	gap timer <milliseconds></milliseconds>	received, it will
<pre></pre>	kill session	Kills command mode session on the Line
no clear line counters Restores the serial counters to the aggregate values.	line <line></line>	
	name <text></text>	Sets the name for this line.
no command mode Disables command mode for the current 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. <li><li>&lt;= number of the terminal line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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 4 (line:4) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed.   <br< td=""></br<>

	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 protocol	Restores the default protocol on the line.
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
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. <li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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 (line:5) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed.   <br< td=""></br<>

	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 protocol	Restores the default protocol on the line.
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
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. <pre><li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li></pre>
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. <pre><li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li></pre>
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 6 (line:6) level commands	
auto show statistics	Continuously displays line statistics.
baud rate bits per second>	Sets the line speed.        

Clears the screen.  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  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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Setting = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Sets be set up to a set up to 0xFF.  Sets boot-up wait time for command mode serial string.  Sets be set with possible binary characters.  Sets be default and the current value of settings.  Sets be factory to default of no flow control.  Restores the default on the line.  Sets the name defa</milliseconds>		Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
Sets the current line to always be in command mode.  command mode echo serial string disable  command mode echo serial string enable  Enables 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 defined serial boot string to be echoed in the CLI.  Enables 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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode signon message string.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Enables user-to what time for command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode serial string.  Sets boot-up wait time for data on the line.  Uses seven bits for data on the line.  Sets seven bits for data on the line.  Sets the default for no flow control.  Restores the default of no parity.  Restores the default of no parity.  Restores the default p	clear line counters	Sets the serial counters to zero.
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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Settings = text with possible binary characters.  Within    use binary decimal up to 255 or hex up to 0xFF.  Within    use binary decimal up to 255 or hex up to 0xFF.  Within    use binary decimal up to 255 or hex up to 0xFF.  Within    use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Individual time command mode seria	clrscrn	Clears the screen.
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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets to sign-on message that is sent from the serial port when the line is in command mode.  Sets boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 255 or hex up to 0xFF.  Within I use binary decimal up to 25	command mode always	Sets the current line to always be in command mode.
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.  strings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  sstrings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  millisecondss – wait time.  configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  default baud rate  default data bits  Restores the default speed of 9600 bits per second.  default flow control  Restores the default of eight data bits.  default flow control  Restores the default of no flow control.  Restores the default for no flow control.  Restores the default protocol on the line.  default stop bits  Restores the default of no parity.  default protocol  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop bits  Restores the default of one parity.  default trop b	command mode echo serial string disable	
command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string = text with possible binary characters. Within {} specify decimal milliseconds time delay.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  sating = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. will seconds = wait time.  Configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven 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.  Restores the default of no parity.  default parity  Restores the default of no parity.  default protocol  Restores the default for no parity.  default threshold  Restores the default for no stop bit.  Restores the default tone stop bit.  Restores the default speed on the line.  default wor char  Restores the default wor character on this line.  Restores the default wor character on this line.  Exits to the enable level  liow control hardware  Uses nardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  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  Enters the line level.  eline < line > line = l	command mode echo serial string enable	
command mode.  saftring> = lext with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] specify decimal milliseconds time delay.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  saftring> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven 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 parity  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default for one stop bit.  Restores the default for control one the line.  default threshold  Restores the default for control on the line.  default two character on this line.  Desire the default worf character on this line.  Desire the default worf character on this line.  Desire the default worf character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Does not provide flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff character) flow control on the line.  Does not provide flow control on the line.  Does not provide flow control on the line.  Does not provide flow control on the line.  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 c	command mode serial string	_
when the device boots and when the line is in command mode. <pre></pre>	command mode serial string <string></string>	command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
<milliseconds> = wait time. 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 seight 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 protocol Restores the default protocol on the line. default threshold Restores the default protocol on the stop bit. Restores the default of one stop bit. Restores the default worf character on this line. default xoff char Restores the default xoff character on this line. default xon char Restores the default xon character on this line. Exits to the enable level Illow control hardware Uses hardware (RTS/CTS) flow control on the line. Illow control none Does not provide flow control on the line. Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) flow control on the line. Uses software (xon/xoff characters) flow control on the line. 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 Enters the line level. Aline&gt; = number of the line (serial port) to be configured. Name &lt; text&gt; Sets the name for this line. Restores the serial counters to the aggregate values.</milliseconds>	command mode signon message <string></string>	when the device boots and when the line is in command mode. <string> = text with possible binary characters.</string>
data bits 7  Uses seven bits for data on the line.  data bits 8  Uses eight bits for data on the line.  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 protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of no stop bit.  Restores the default of no stop bit.  Restores the default for one stop bit.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default work of character on this line.  Restores the default protocol on the line.  Uses hardware (RTS/CTS) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.    Ine> = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.	command mode wait time <milliseconds></milliseconds>	
data bits 8  Uses eight bits for data on the line.  default baud rate  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 no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of none stop bit.  Restores the default of none stop bit.  Restores the default woff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Source on the line.  Source of the wontrol none on the line.  Source on the line in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In eline > In enters the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	configure current settings	Configures line with the current value of settings.
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 no parity.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default word of character on this line.  Restores the default xoff character on this line.  Restores the default xor character on this line.  Restores the default concharacter on this line.  Lexit to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inner <="" li="">Inner &lt; li&gt;Inner &lt; line &lt; li&gt;Inner &lt; line &lt; li&gt;Inner &lt; line &lt; li&gt;Inner &lt; li</inner>	data bits 7	Uses seven bits for data on the line.
Restores the default of eight data bits.  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Exits to the enable level  I Uses hardware (RTS/CTS) flow control on the line.  Row control none  Does not provide flow control on the line.  Does not provide flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  I ine > = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.	data bits 8	Uses eight bits for data on the line.
default flow control  default parity  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default control control control line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the gap timer (anilose control on the line.  Sets the gap timer (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <ine> <ine> <ine>    Anime <text>  Sets the name for this line.   Anone <text>  Sets the serial counters to the aggregate values.</text></text></ine></ine></ine>	default baud rate	Restores the default speed of 9600 bits per second.
Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Restores the default xon character on this line.  Exits to the enable level  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inne>  Enters the line level.  <ine>  Inne &lt; line&gt;  Restores the serial counters to the aggregate values.</ine></inne>	default data bits	Restores the default of eight data bits.
Restores the default protocol on the line.  default stop bits  Restores the default of one stop bit.  Restores the default threshold.  Restores the default xoff char default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <ine> <ine< <ine=""> <ine> <ine> <ine> <ine> <ine> <ine> <ine> <ine> <ine> <i< td=""><td>default flow control</td><td>Restores the default of no flow control.</td></i<></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine<></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></ine>	default flow control	Restores the default of no flow control.
Restores the default of one stop bit.  Restores the factory default threshold.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Luses hardware (RTS/CTS) flow control on the line.  Row control none  Does not provide flow control on the line.  Luses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In eline > Enters the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default parity	Restores the default of no parity.
Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solution (RTS/CTS) flow control on the line.  Solution (RTS/CTS) flow control o	default protocol	Restores the default protocol on the line.
Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solution control hardware  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Solution control software  Solution control software  Solution control software  Uses software (xon/xoff characters) flow control on the line.  Solution control software in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline < line > = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default stop bits	Restores the default of one stop bit.
Restores the default xon character on this line.  Exit Exits to the enable level  flow control hardware  flow control none  flow control software  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li></milliseconds>	default threshold	Restores the factory default threshold.
Exits to the enable level  Glow control hardware  Glow control none  Glow control software  Glow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline > In cline sounters  Glow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline > In cline serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default xoff char	Restores the default xoff character on this line.
flow control hardware  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li>&lt;= number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li></milliseconds>	default xon char	Restores the default xon character on this line.
Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li></li></li></li>	exit	Exits to the enable level
Illuses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li>&lt; = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li>	flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
line.     gap timer <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 <li>line <li>line &gt;   Enters the line level.     <li>  <li>  &lt;     = number of the line (serial port) to be configured.     sets the name for this line.     Restores the serial counters to the aggregate values.  </li></li></li></li></milliseconds>	flow control none	Does not provide flow control on the line.
received, it will be forwarded after this time since the last character.  kill session  Kills command mode session on the Line  Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li>	flow control software	1
Enters the line level. <ine> = number of the line (serial port) to be configured.  name <text> Sets the name for this line.  Restores the serial counters to the aggregate values.</text></ine>	gap timer <milliseconds></milliseconds>	received, it will
<pre></pre>	kill session	Kills command mode session on the Line
no clear line counters Restores the serial counters to the aggregate values.	line <line></line>	
	name <text></text>	Sets the name for this line.
no command mode Disables command mode for the current 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. <pre><li><li>&lt;= number of the terminal line (serial port) to be configured.</li></li></pre>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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 7 (line:7) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed.   <br< td=""></br<>

Clears the screen.  Clears the screen.  Command mode always  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.  Command mode echo serial string enable  Enables user of enter a custom string at boot time to enter command mode.  Command mode serial string  Command mode serial string  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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode serial string characters.  Within [] use binary decimal unit to 255 or hex up to 0xFF. Within [] specify decimal milliseconds time delay.  Sets a stign-on message that is sent from the serial port when the line is in command mode existing— text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Configure current settings  Configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  Sets bot-up wait time for command mode serial string.  Configure current settings  Configures line with the current value of settings.  data bits 8  Uses eight bits for data on the line.  Setable bits 6  Setable setable 1  Setabl		Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
Sets the current line to always be in command mode.  command mode echo serial string disable bisables 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 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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal with the serial port when the device boots and when the line is in command mode.  «strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  configure current settings  Configures line with the current value of settings.  Ideal bits 7  Uses seven bits for data on the line.  Uses seven bits for data on the line.  Ideal bits 8  Uses seven bits for data on the line.  Ideal bits 9  Getault data bits  Restores the default of plow control.  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default tone stop bit.  Restores the default protocol on the line.  Restores the default work character on this line.  Restores the default work ch</milliseconds>	clear line counters	Sets the serial counters to zero.
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.  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    use binary decimal up to 255 or hex up to 0XF	clrscrn	Clears the screen.
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.  Command mode serial string  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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets to sign-on message that is sent from the serial port when the line is in command mode.  Sets boots and when the line is in command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  Individual time for command mode serial string.  Sets boot-up wait time for command mode serial string.  Individual to a serial string that a serial port when the current value of settings.  Sets boot-up wait time for command mode serial string.  Individual to a serial string that a serial port when the current value of settings.  Sets be seven bits for data on the line.  Sets be seried bits for data on the line.  Sets be default and the current value of settings.  Set before the default of eight data bits.  Setable to the default of the current value of settings.  Set before the default of no flow control.  Sets default flow control  Restores the default of no low control.  Sets default the shold  Restores the default of no low control.  Sets the default to no estop bit.  Set and threshold  Restores the default to no estop bit.  Set and threshold  Restores the default to no haracter on this line.  Set to the enable	command mode always	Sets the current line to always be in command mode.
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.  Sets a string that can be entered at boot time to enter command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] specify decimal milliseconds time delay.  Decommand mode signon message <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.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  milliseconds = wait time.  Configures line with the current value of settings.  Configures line with the current value of settings.  Configures line with the current value of settings.  Clata bits 7  Uses seven bits for data on the line.  Idefault baud rate  Restores the default speed of 9600 bits per second.  Restores the default of eight data bits.  Clefault flow control  Restores the default of no flow control.  Restores the default of no flow control.  Restores the default protocol on the line.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default to one character on this line.  Restores the default to one character on this line.  Restores the default to one character on this line.  Restores the default to one control on the line.  Does not provide flow control on the line.  Sets to the enable level  Row control hardware  Low control hardware  Low control hardware  Low control hardware  Low control one  Does not provide flow control on the line.  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  Kill session  Kill session the line (serial port) to be conf</string>	command mode echo serial string disable	
command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string be text with possible binary characters. Within {} specify decimal milliseconds time delay.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string. Within [] use binary decimal milliseconds.  Restores the default of no flow control.  Restores the default of no flow control on the line.  Sets the default to perfect the perfect of 9600 bits per second.  Restores the default protocol on the line.  Sets the enable level  Sets the enable level  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	command mode echo serial string enable	
command mode.  saftring> = lext with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] specify decimal milliseconds time delay.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  saftring> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  configure current settings  Configures line with the current value of settings.  data bits 7  Uses seven bits for data on the line.  default baud rate  Restores the default speed of 9600 bits per second.  Restores the default speed of 9600 bits per second.  Restores the default for no flow control.  default flow control  Restores the default of no parity.  default parity  Restores the default of no parity.  default parity  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default speed of 9600 bits ine.  default threshold  Restores the default for control.  default threshold  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default speed on the line.  default threshold  Restores the default soft character on this line.  default two character on this line.  Exist to the enable level  Uses hardware (RTS/CTS) flow control on the line.  low control hardware  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  By the part of the line series on the line.  Will session  Kill session  Kill session  Kill session the line (serial port) to be configured.	command mode serial string	1
when the device boots and when the line is in command mode. <pre></pre>	command mode serial string <string></string>	command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
milliseconds> = wait time.	command mode signon message <string></string>	when the device boots and when the line is in command mode. <pre><string> = text with possible binary characters.</string></pre>
data bits 7  Uses seven bits for data on the line.  data bits 8  Uses eight bits for data on the line.  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 protocol on the line.  Restores the default of no stop bit.  Restores the default word of the line.  Restores the default word on the line.  Restores the default word character on this line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.    Ine> = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.	command mode wait time <milliseconds></milliseconds>	
data bits 8  Uses eight bits for data on the line.  default baud rate  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 no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of none stop bit.  Restores the default of none stop bit.  Restores the default woff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Source on the line.  Source of the wontrol none on the line.  Source on the line in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In eximple of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	configure current settings	Configures line with the current value of settings.
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 no parity.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default was the default threshold.  Restores the default was the default threshold.  Restores the default was the	data bits 7	Uses seven bits for data on the line.
Restores the default of eight data bits.  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Exits to the enable level  I Uses hardware (RTS/CTS) flow control on the line.  Row control none  Does not provide flow control on the line.  Does not provide flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  I ine > = number of the line (serial port) to be configured.  Restores the serial counters to the aggregate values.	data bits 8	Uses eight bits for data on the line.
default flow control  default parity  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default control control control line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the gap timer (anilose control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In extended after this line (serial port) to be configured.  Restores the serial counters to the aggregate values.	default baud rate	Restores the default speed of 9600 bits per second.
Restores the default of no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Restores the default xon character on this line.  Exits to the enable level  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inne>  Enters the line level.  <ine>  Inne &lt; line&gt;  Restores the serial counters to the aggregate values.</ine></inne>	default data bits	Restores the default of eight data bits.
Restores the default protocol on the line.  default stop bits  Restores the default of one stop bit.  Restores the default threshold.  Restores the default xoff char default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  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.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <inex> line &lt; line &gt; line &lt; set the serial counters to the aggregate values.</inex>	default flow control	Restores the default of no flow control.
Restores the default of one stop bit.  Restores the factory default threshold.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Luses hardware (RTS/CTS) flow control on the line.  Row control none  Does not provide flow control on the line.  Luses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In eline > Enters the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default parity	Restores the default of no parity.
Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solution (RTS/CTS) flow control on the line.  Solution control none  Does not provide flow control on the line.  Solution control software  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff characters) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control software (xon/xoff character) flow control on the line.  Solution control solution control solution control on the line.  Solution control solution control solution control on the line.  Solution	default protocol	Restores the default protocol on the line.
Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solution control hardware  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Solution control software  Solution control software  Solution control software  Uses software (xon/xoff characters) flow control on the line.  Solution control software in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline < line > = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default stop bits	Restores the default of one stop bit.
Restores the default xon character on this line.  Exit Exits to the enable level  flow control hardware  flow control none  flow control software  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li></milliseconds>	default threshold	Restores the factory default threshold.
Exits to the enable level  Glow control hardware  Glow control none  Glow control software  Glow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline > In cline serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.	default xoff char	Restores the default xoff character on this line.
flow control hardware  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li>&lt;= number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li></milliseconds>	default xon char	Restores the default xon character on this line.
Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li></li></li></li>	exit	Exits to the enable level
Illuses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <li><li><li><li>&lt; = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li></li></li></li>	flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
line.     gap timer <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 <li>line <li>line &gt;</li></li></milliseconds>	flow control none	Does not provide flow control on the line.
received, it will be forwarded after this time since the last character.  kill session  Kills command mode session on the Line  Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.  Restores the serial counters to the aggregate values.</li>	flow control software	1
Enters the line level. <ine> = number of the line (serial port) to be configured.  name <text> Sets the name for this line.  Restores the serial counters to the aggregate values.</text></ine>	gap timer <milliseconds></milliseconds>	received, it will
<pre></pre>	kill session	Kills command mode session on the Line
no clear line counters Restores the serial counters to the aggregate values.	line <li>line&gt;</li>	
	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	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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
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 <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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 8 (line:8) level commands	
auto show statistics	Continuously displays line statistics.
baud rate bits per second>	Sets the line speed.          Sets the line speed.  

Clears the screen.  Clears the screen.  Command mode always  Sets the current line to always be in command mode.  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-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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Settings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  Configures line with the current value of settings.  Configures the default of eight data on the line.  Configures the default of no flow control.  Restores the default of no flow control.  Restores the default of no parity.  Restores the default protocol on the line.  Configures the default for hor parity.  Restores the default of no hor parity.  Restores the default of no hor parity.  Restores the default of hor parity.  Re</milliseconds>		Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
Sets the current line to always be in command mode.  command mode echo serial string disable the CLI.  Command mode echo serial string enable Enables user-defined serial boot string to be echoed in the CLI.  Command mode 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>  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.  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.  Command mode wait time <*milliseconds> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <*milliseconds> = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Command mode wait time <*milliseconds> = wait time.  **Sets boot-up wait time for command mode serial string.**  **milliseconds> = wait time.  **Configures line with the current value of settings.  data bits 7	clear line counters	Sets the serial counters to zero.
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.  Sets a string that can be entered at boot time to enter command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] so binary decimal up to 255 or hex up to 0xFF.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets a sign-on message that is sent from the serial port when the line is in command mode.  strings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets as sign-on message that is sent from the serial port when the device boots and when the line is in command mode existings = text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Sets boot-up wait time for command mode serial string.  command mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode wait time serial port when the line is in command mode serial string.  command mode serial string serial port when the line serial</milliseconds>	clrscrn	Clears the screen.
the CLI.  Command mode echo serial string enable  Enables user to enter a custom 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.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a string that can be entered at boot time to enter command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.  Sets boot-up wait time for command mode serial string.  Configure current settings  Configure current settings  Configures line with the current value of settings.  Uses seven bits for data on the line.  Uses seven bits for data on the line.  Uses seven bits for data on the line.  Restores the default speed of 9600 bits per second.  default baud rate  Restores the default of eight data bits.  default flow control  Restores the default of no flow control.  Restores the default for no flow control.  Restores the default protocol on the line.  default protocol  Restores the default of no parity.  default protocol  Restores the default of one stop bit.  Restores the default vor character on this line.  default two char  Restores the default vor character on this line.  Exit to the enable level  Sexit to the enable level  Uses software (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (RTS/CTS) flow control on the line.  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  Kill session  Lines = Innumber of the line (serial port) to be configured.	command mode always	Sets the current line to always be in command mode.
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.  Sets a string that can be entered at boot time to enter command mode.  Strings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Within [] specify decimal impliesconds time delay.  Command mode signon message <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.  Strings – text with possible binary characters.  Within [] use binary decimal up to 255 or hex up to 0xFF.  Dommand mode wait time <milliseconds>  Sets boot-up wait time for command mode serial string.  Configure current settings  Configures line with the current value of settings.  Duses seven bits for data on the line.  Uses seven bits for data on the line.  Uses seight bits for data on the line.  Default bauf rate  Restores the default speed of 9600 bits per second.  Restores the default of eight data bits.  Restores the default of no parity.  Default parity  Restores the default of no parity.  Default parity  Restores the default of no parity.  Default protocol  Restores the default of no parity.  Default protocol  Restores the default of no parity.  Default protocol  Restores the default to fone stop bit.  Restores the default of none stop bit.  Restores the default son character on this line.  Restores the default son chara</milliseconds></string>	command mode echo serial string disable	
command mode.  Sets a string that can be entered 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 {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal my to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal up to 255 or hex up to 0xFF. Within {} specify decimal my to 0xFF. Within {} s	command mode echo serial string enable	
command mode. <asting> text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within [] use binary decimal up to 255 or hex up to 0xFF. Within [] specify decimal milliseconds time delay. Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. ⟨astring&gt; = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.   command mode wait time  ⟨milliseconds&gt; = wait time for command mode serial string. ⟨milliseconds&gt; = wait time.   configure current settings Configures line with the current value of settings. data bits 7   data bits 7 Uses seven 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 parity.   default parity Restores the default of no parity.   default protocol Restores the default protocol on the line.   default stop bits Restores the default protocol on the line.   default threshold Restores the default of one stop bit.   default won char Restores the default won character on this line.   default xon char Restores the default xon character on this line.   exit Exits to the enable level   llow control hardware Uses software (xon/xoff characters) flow control on the line.   flow control software Uses software (xon/xoff characters) flow control on the line.   gap timer <milliseconds> Sets the gap timer in milliseconds. If some data has been received, it will be forwarded</milliseconds></asting>	command mode serial string	, , , , , , , , , , , , , , , , , , ,
when the device boots and when the line is in command mode. <pre></pre>	command mode serial string <string></string>	command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.</string>
<milliseconds> = wait time. 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 protocol Restores the default protocol on the line. default stop bits Restores the default of one stop bit. Restores the default of one stop bit. Restores the default wof character on this line. default woff char default woff character on this line. default xon char Restores the default xon character on this line. default xon char Restores the default xon 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. Does not provide flow control on the line. Glow control software Uses software (xon/xoff characters) flow control on the line. Gets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character. Kills command mode session on the Line Enters the line level. Inex = number of the line (serial port) to be configured. Sets the name for this line.</milliseconds>	command mode signon message <string></string>	when the device boots and when the line is in command mode. <string> = text with possible binary characters.</string>
data bits 7  data bits 8  default baud rate  default baud rate  default data bits  default flow control  default protocol  default treshold  default word char  default stop bits  default word char  default word character on this line.  default word character on this line.  Exits to the enable level  down control hardware  flow control none  Does not provide flow control on the line.  duses software (xon/xoff characters) flow control on the line.  default will be forwarded after this time since the last character.  kill session  kills command mode session on the Line  Enters the line level. <input <p="" served.=""/> In word of the line (serial port) to be configured.  Sets the name for this line.	command mode wait time <milliseconds></milliseconds>	
data bits 8  Uses eight bits for data on the line.  default baud rate  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 no parity.  Restores the default protocol on the line.  Restores the default protocol on the line.  Restores the default of none stop bit.  Restores the default of none stop bit.  Restores the default woff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  flow control hardware  Uses hardware (RTS/CTS) flow control on the line.  flow control software  Uses software (xon/xoff characters) flow control on the line.  Gap time <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <li><li><li><li><li></li><li><li></li><li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li>&lt;</li></li></li></li></li></li></milliseconds>	configure current settings	Configures line with the current value of settings.
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 no parity.  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the default was default threshold.  Restores the default was character on this line.  Exits to the enable level  flow control hardware  Restores the default was character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Gap timer <milliseconds>  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <inne>  Enters the line level.  <ine>  Enters the line (serial port) to be configured.</ine></inne></milliseconds>	data bits 7	Uses seven bits for data on the line.
default data bits  default flow control  default parity  default protocol  default stop bits  default work control  default work control  Restores the default of no parity.  Restores the default protocol on the line.  default stop bits  default threshold  default work char  Restores the default work character on this line.  Exits to the enable level  flow control hardware  flow control hardware  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <ine> </ine></ine></ine></ine></ine></ine></ine></ine></ine></ine></milliseconds>	data bits 8	Uses eight bits for data on the line.
default flow control  default parity  default protocol  default protocol  default stop bits  default treshold  default word char  default word character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  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  Enters the line level. <inne> = number of the line (serial port) to be configured.  Sets the name for this line.</inne>	default baud rate	Restores the default speed of 9600 bits per second.
default parity  default protocol  default stop bits  default threshold  default xoff char  default xon char  exit  flow control none  flow control software  flow control software  gap timer <milliseconds>  Sets the gap timer in milliseconds.  Kills command mode session on the Line  Enters the line (serial port) to be configured.  Restores the default of one stop bit.  Restores the default threshold.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <inex -="" -<="" exit="" td=""><td>default data bits</td><td>Restores the default of eight data bits.</td></inex></milliseconds>	default data bits	Restores the default of eight data bits.
default protocol  Restores the default protocol on the line.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default xon character on this line.  Exits to the enable level  Flow control hardware  Restores the default von character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Uses not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  <  Ine>	default flow control	Restores the default of no flow control.
Restores the default of one stop bit.  Restores the default of one stop bit.  Restores the factory default threshold.  Restores the default xoff character on this line.  Restores the default xor character on this line.  Restores the default xon character on this line.  Exits to the enable level  Solve control hardware  Uses hardware (RTS/CTS) flow control on the line.  Solve control software  Uses software (xon/xoff characters) flow control on the line.  Solve control software  Uses software (xon/xoff characters) flow control on the line.  Solve 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  Enters the line level. <inne> enumber of the line (serial port) to be configured.  Sets the name for this line.</inne>	default parity	Restores the default of no parity.
default threshold  default xoff char  default xoff char  Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Illuses hardware (RTS/CTS) flow control on the line.  Illuses software (xon/xoff characters) flow control on the line.  Illuses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <inner <="" li="">Inner &lt; line &gt; = number of the line (serial port) to be configured.  Sets the name for this line.</inner>	default protocol	Restores the default protocol on the line.
Restores the default xoff character on this line.  Restores the default xon character on this line.  Restores the default xon character on this line.  Exits to the enable level  Uses hardware (RTS/CTS) flow control on the line.  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level. <incenter (serial="" be="" configured.="" for="" line="" line.<="" name="" of="" port)="" sets="" td="" the="" this="" to=""><td>default stop bits</td><td>Restores the default of one stop bit.</td></incenter>	default stop bits	Restores the default of one stop bit.
Restores the default xon character on this line.  Exit Exits to the enable level  Glow control hardware  Glow control none  Glow control software  Glow control on the line.  Glow control software  Glow control on the line.  Glow control on the line.  Gets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  In cline > = number of the line (serial port) to be configured.  Sets the name for this line.	default threshold	Restores the factory default threshold.
Exits to the enable level  flow control hardware  flow control none  flow control none  flow control software  flow control software  gap timer <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  Enters the line level.  <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li></milliseconds>	default xoff char	Restores the default xoff character on this line.
flow control hardware  flow control none  flow control none  flow control software  flow control software  Grow control software  flow control software  Grow control software  Grow control software  Grow control software  Uses software (xon/xoff characters) flow control on the line.  Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.  Kills command mode session on the Line  Enters the line level.  Ine> = number of the line (serial port) to be configured.  Sets the name for this line.	default xon char	Restores the default xon character on this line.
flow control none  Does not provide flow control on the line.  Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.</li></li></li></li></milliseconds>	exit	Exits to the enable level
I Uses software (xon/xoff characters) flow control on the line.  gap timer <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  Enters the line level.  <li><li><li><li>= number of the line (serial port) to be configured.  Sets the name for this line.</li></li></li></li></milliseconds>	flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
line.   gap timer <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 &lt; line &gt;</milliseconds>	flow control none	Does not provide flow control on the line.
received, it will be forwarded after this time since the last character.  kill session  Kills command mode session on the Line  Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.</li>	flow control software	1
line <li>line &gt; Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.  Sets the name for this line.</li></li>	gap timer <milliseconds></milliseconds>	received, it will
<pre><li><li>&lt; = number of the line (serial port) to be configured.</li></li></pre> name <text> Sets the name for this line.</text>	kill session	Kills command mode session on the Line
	line <line></line>	
no clear line counters Restores the serial counters to the aggregate values.	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	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. <li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li>
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. <pre><li><li>&lt; = number of the tunnel line (serial port) to be configured.</li></li></pre>
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 9 (line:9) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <bits per="" second=""></bits>	Sets the line speed.          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 protocol	Restores the default protocol on the line.
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
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. <li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li>
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 <li>line&gt;</li>	Enters the tunnel level. <li><pre><li><pre><li>= number of the tunnel line (serial port) to be configured.</li></pre></li></pre></li>
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 commands	
clrscrn	Clears the screen.
default duplex	Restores the default duplex setting, which is auto.
default speed	Restores the default speed setting, which is auto-

	nogotiato
dupley oute	negotiate.
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 auto-negotiate.
write	Stores the current configuration in permanent memory.
link (config-ethernet:eth1) level commands	
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 auto-negotiate.
write	Stores the current configuration in permanent memory.
link (config-ethernet:eth0) level commands	
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.
	Sets the speed of the Ethernet link to auto-negotiate.
speed auto	joets the speed of the Ethernet link to auto-negotiate.

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.
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.
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 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.
<u> </u>	I .

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.
Willo	Stores the current configuration in permanent memory.
modem (tunnel-modem:13) level commands	Stores the current configuration in permanent memory.
	Clears the screen.
modem (tunnel-modem:13) level commands	
modem (tunnel-modem:13) level commands clrscrn	Clears the screen.  Sets the CONNECT string used in modem emulation.
modem (tunnel-modem:13) level commands clrscrn connect string <text></text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.</string>
modem (tunnel-modem:13) level commands clrscrn connect string <text>  default incoming connection default response type</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem com-</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  echo pluses enable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  echo pluses enable  error unknown commands disable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  echo pluses enable  error unknown commands disable  error unknown commands enable</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  echo pluses enable  error unknown commands disable  error unknown commands enable  exit</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns to the tunnel level.</string>
modem (tunnel-modem:13) level commands  clrscrn  connect string <text>  default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  error unknown commands disable  error unknown commands enable  exit  incoming connection automatic</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.</string>
clrscrn connect string <text>  default incoming connection default response type display remote ip disable display remote ip enable  echo commands disable echo commands enable echo pluses disable echo pluses enable  error unknown commands disable error unknown commands enable exit incoming connection automatic incoming connection disabled</text>	Clears the screen.  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming</string>

	dem emulation.
reassert	Asserts tunnel modem status with current configured val-
	ues.
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 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:9) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation. <string> = connect string.</string>
connect string <text>  default incoming connection</text>	
-	<string> = connect string.</string>
default incoming connection	<pre><string> = connect string.  Default disables incoming network connections.</string></pre>
default incoming connection default response type	<pre><string> = connect string.  Default disables incoming network connections.  Default uses text type responses.</string></pre>
default incoming connection default response type display remote ip disable	<pre><string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the</string></pre>
default incoming connection default response type display remote ip disable display remote ip enable	<pre><string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.</string></pre>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands.</string>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable echo commands enable	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands. Echoes modem commands. Does not echo the +++ characters when entering modem</string>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable	<pre><string> = connect string.  Default disables incoming network connections.  Default uses text type responses.  The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem com-</string></pre>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable	<pre></pre>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands. Echoes modem commands. Does not echo the +++ characters when entering modem command mode. Echoes the +++ characters when entering modem command mode. Returns OK on unknown AT commands.</string>
default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  echo pluses enable  error unknown commands disable  error unknown commands enable	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands. Echoes modem commands. Does not echo the +++ characters when entering modem command mode. Echoes the +++ characters when entering modem command mode. Returns OK on unknown AT commands. Returns an error upon unknown AT commands.</string>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands. Echoes modem commands. Does not echo the +++ characters when entering modem command mode. Echoes the +++ characters when entering modem command mode. Returns OK on unknown AT commands. Returns an error upon unknown AT commands. Returns to the tunnel level.</string>
default incoming connection default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable error unknown commands enable exit incoming connection automatic	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands. Echoes modem commands. Does not echo the +++ characters when entering modem command mode. Echoes the +++ characters when entering modem command mode. Returns OK on unknown AT commands. Returns an error upon unknown AT commands. Returns to the tunnel level. Automatically answer incoming network connections.</string>
default incoming connection  default response type  display remote ip disable  display remote ip enable  echo commands disable  echo commands enable  echo pluses disable  echo pluses enable  error unknown commands disable  error unknown commands enable  incoming connection automatic  incoming connection disabled	<string> = connect string. Default disables incoming network connections. Default uses text type responses. The incoming RING has nothing following it. The incoming RING is followed by the IP address of the caller. Does not echo modem commands. Echoes modem commands. Does not echo the +++ characters when entering modem command mode. Echoes the +++ characters when entering modem command mode. Returns OK on unknown AT commands. Returns an error upon unknown AT commands. Returns to the tunnel level. Automatically answer incoming network connections. Disable incoming network connections. Wait for an ATA command before answering an incoming</string>

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:8) level commands	<u> </u>
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:7) level commands	
clrscrn	Clears the screen.
connect string <text></text>	Sets the CONNECT string used in modem emulation.
<u> </u>	

	<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 enable	Poturno an arrar unan unknown AT commanda
exit	Returns an error upon unknown AT commands.  Returns to the tunnel level.
incoming connection automatic incoming connection disabled	Automatically answer incoming network connections.  Disable incoming network connections.
incoming connection disabled	Wait for an ATA command before answering an incoming
Incoming connection manual	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.
	Default uses text type responses. The incoming RING has nothing following it.
default response type	
default response type display remote ip disable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the
default response type display remote ip disable display remote ip enable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.
default response type display remote ip disable display remote ip enable echo commands disable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem com-
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable error unknown commands enable exit	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit incoming connection automatic	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit incoming connection automatic incoming connection disabled incoming connection manual	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit incoming connection automatic incoming connection disabled	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit incoming connection automatic incoming connection disabled incoming connection manual	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for mo-
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit incoming connection automatic incoming connection disabled incoming connection manual	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  Asserts tunnel modem status with current configured val-
default response type display remote ip disable display remote ip enable echo commands disable echo commands enable echo pluses disable echo pluses enable error unknown commands disable error unknown commands enable exit incoming connection automatic incoming connection disabled incoming connection manual no connect string reassert	The incoming RING has nothing following it.  The incoming RING is followed by the IP address of the caller.  Does not echo modem commands.  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  Asserts tunnel modem status with current configured values.

show status  Displays turnel modern status.  verbose response disable  Does not send Modern Response Codes.  Sends Modern Response Codes out on the Serial Line.  Stores the current configuration in permanent memory.  modern (tunnel-modem:4) level commands  cliscin  Clears the screen.  Clears the screen.  Sets the CONNECT string used in modern emulation.  -strings = connect string.  default incoming connection  default response type  Default disables incoming network connections.  default response type  Default disables incoming network connections.  default response type  Default disables incoming network connections.  default remove ip enable  The incoming RING has nothing following it.  display remote ip enable  caller.  echo commands disable  Does not echo medem commands.  echo pluses disable  Does not echo the +++ characters when entering modern command mode.  echo pluses disable  Echoes the +++ characters when entering modern command mode.  echo pluses enable  Echoes the +++ characters when entering modern command mode.  echo pluses enable  Echoes the outpoun unknown AT commands.  error unknown commands disable  Returns OK on unknown AT commands.  exit  Returns an error upon unknown AT commands.  exit  Returns to the tunnel level.  incoming connection automatic  incoming connection manual  Wait for an ATA command before answering an incoming network connections.  incoming connection manual  Wait for an ATA commands with current configured values.  Persponse type numeric  Uses numeric type responses.  show  Displays the last 20 commands entered during the current configured values.  Possible incoming modern configuration.  Possible incoming entwork connection.  Possible incoming entwork connections.  Possible incoming entwork connections.  Possible incoming entwork connection.  Possible incoming entwork connections.  Possible incoming network connections.  Possible incoming entwork connections.  Possible incoming entwork connections.  Possible incoming entwork connections.  Possible incoming entwork connect	show history	Displays the last 20 commands entered during the current CLI session.
verbose response disable  verbose response enable  Sends Modem Response Codes out on the Serial Line.  Sends Modem Response Codes out on the Serial Line.  Sends Modem Response Codes out on the Serial Line.  Sends Modem Response Codes out on the Serial Line.  Sets the current configuration in permanent memory.  Connect string <a href="#"></a>	show status	
verbose response enable write Stores the current configuration in permanent memory.  modem (tunnel-modem:4) level commands  cirsorn Clears the screen.  Clears the screen.  Clears the screen.  Connect string <text> Sets the CONNECT string used in modem emulation. <string>= connect string, leven'x connections.  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.  The incoming RING is followed by the IP address of the caller.  echo commands disable Does not echo 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 OK on unknown AT commands.  exit Returns to the tunnel level.  incoming connection automatic Automatically answer incoming network connections.  incoming connection manual Wait for an ATA command before answering an incoming network connections.  incoming connection manual  Passerts tunnel modem status with current configured values.  response type numeric Uses numeric type responses.  Passerts tunnel modem status with current configured values.  Passerts unnel modem status.  Displays the last 20 commands entered during the current CLI session.  Show status Displays tunnel modem Response Codes.  Possors type numer condement of the service of the service of the service of the service of the service.  Passert String = connect of the current configuration in permanent memory.  Passerts the connect string used in modem emulation.  Show status Displays the last 20 commands entered during the current configuration in permanent memory.  Passerts the connect string used in modem emulation.  Sets the connect string used in modem emulation.  Sets the connect string under modem emulation.  Sets the connect string used in modem emulat</string></text>	verbose response disable	
write Stores the current configuration in permanent memory.  modern (tunnel-modem:4) level commands  cirscm  Clears the screen.  Connect string <fext> Sets the CONNECT string used in modem emulation.</fext>	-	·
cirsorn Clears the screen. Connect string < text> Sets the CONNECT string used in modem emulation. <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.</a> <a href="#">Sets the CONNECT string used in modem emulation.<!--</td--><td></td><td>·</td></a>		·
Clears the screen.	modem (tunnel-modem:4) level commands	
estring> = connect string.		Clears the screen.
default response type  display remote ip disable  The incoming RING has nothing following it.  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 OK on unknown AT commands.  exit  Returns to the tunnel level.  incoming connection automatic  incoming connection disabled  Disable incoming network connections.  incoming connection manual  Wait for an ATA command before answering an incoming network connections.  incoming connection manual  Wait for an ATA command before answering an incoming network connections.  incoming connection was placed and the membrane placed was placed and the membrane placed was placed and the placed was placed was placed and the placed was placed and the placed was placed was placed and the placed was pl	connect string <text></text>	
display remote ip disable  display remote ip enable  The incoming RING is followed by the IP address of the caller.  echo commands disable  Does not echo modem commands.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem commands incoming notwork on unknown AT commands.  Returns to unknown AT commands  Echoes the +++ characters when entering modem commands incoming notwork connections.  Wait for unknown AT commands enteror unknown AT commands enterod promands entered during the current configuration.  Displays the last unnel modem status with current configuration.  Show is presented to present the presented and presented the presented and	default incoming connection	Default disables incoming network connections.
display remote ip enable  cho commands disable  cho commands disable  cho commands enable  cho commands enable  cho pluses disable  cho pluses enable  cror unknown commands disable  cror unknown commands disable  cror unknown commands enable  cror unknown commands  cround enable  cror unknown commands  cround enable  cror unknown at commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  incoming connection disabled  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  cror exponse type numeric  Uses numeric type responses.  show  Displays the current configuration.  blow status blosplays the current configuration.  blow status  Displays the last 20 commands entered during the current CLI session.  show status  verbose response disable  Does not send Modem Response Codes.  cror string send (unnel-modem:3) level commands  clirscrn  Clears the screen.  Clears the screen.  Clears the screen.  Connect string veed in modem emulation.  strings = connect string.  default incoming connection.	default response type	Default uses text type responses.
caller.  ccho commands disable ccho commands enable ccho commands enable ccho pluses disable ccho pluses enable ccho pluses enable ccho pluses enable ccho pluses enable cror unknown commands disable cror unknown commands disable cror unknown commands enable cror unknown commands cror unknown AT commands. Returns an error upon unknown AT commands. cror unknown AT commands.  Returns to the tunnel level. incoming connection automatic incoming connection disabled Disable incoming network connections. incoming connection disabled Disable incoming network connections.  Removes optional CONNECT string information for modem emulation.  Reassert Asserts tunnel modem status with current configured values.  response type numeric Uses numeric type responses.  show Displays the current configuration.  show status 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 commands clirscrn Clears the screen.  Connect string <a href="mailto:center">center ting.</a> Cest the CONNECT string used in modem emulation. <a href="mailto:string-">string-</a> econnect string.  default incoming connection	display remote ip disable	The incoming RING has nothing following it.
echo commands enable  echo pluses disable  cho pluses enable  Echoes modem commands.  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Incoming connection disabled  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  Response type numeric  Uses numeric 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 (funnel-modem:3) level commands  Clears the screen.  Connect string   Clears the screen.  Connect string of text>  Sets the CONNECT string used in modem emulation.  String> = connect string.	display remote ip enable	
echo pluses disable  Does not echo the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Echoes the +++ characters when entering modem command mode.  Error unknown commands disable  Returns OK on unknown AT commands.  Returns an error upon unknown AT commands.  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection and pretwork connection.  Removes optional CONNECT string information for modem emulation.  Reassert  Asserts tunnel modem status with current configured values.  Response type numeric  Uses numeric 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 codes out on the Serial Line.  Write  Stores the current configuration in permanent memory.  modem (tunnel-modem:3) level commands  Clears the screen.  Connect string   Clears the screen.  Connect string on network connections.	echo commands disable	Does not echo modem commands.
command mode.  echo pluses enable  Echoes the +++ characters when entering modem command mode.  error unknown commands disable  error unknown commands enable  Returns OK on unknown AT commands.  error unknown commands enable  Returns a 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.  Removes optional CONNECT string information for modem emulation.  reassert  Asserts tunnel modem status with current configured values.  response type numeric  Uses numeric type responses.  show  Displays the current configuration.  bisplays 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 commands  clears the screen.  Clears the screen.  Clears the screen.  Sets the CONNECT string used in modem emulation. <a href="https://wintex.pdf"></a> Sets the CONNECT string used in modem emulation.	echo commands enable	Echoes modem commands.
mand mode.  error unknown commands disable error unknown commands enable error unknown commands enable exit Returns to the tunnel level. incoming connection automatic incoming connection disabled Disable incoming network connections. Disable incoming network connections. Disable incoming network connections. Disable incoming network connections. Incoming connection manual Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  reassert Asserts tunnel modem status with current configured values.  response type numeric Uses numeric 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.  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 commands clarscrn Clears the screen.  Clears the screen.  Clears the screen.  Cennect string used in modem emulation.  string> = connect string. Default disables incoming network connections.	echo pluses disable	
error unknown commands enable exit  Returns to the tunnel level.  Automatically answer incoming network connections.  Disable incoming network connections.  Incoming connection disabled  Disable incoming network connections.  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  reassert  Asserts tunnel modem status with current configured values.  response type numeric  Uses numeric 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.  Perbose 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 commands  clirscrn  Clears the screen.  Clears the screen.  Connect string < text>  Sets the CONNECT string used in modem emulation. <string> = connect string.  Default disables incoming network connections.</string>	echo pluses enable	
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 commands  clrscrn Clears the screen.  Connect string <text> Clears the screen.  Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connections.</string></text>	error unknown commands disable	Returns OK on unknown AT commands.
incoming connection automatic incoming connection disabled Disable incoming network connections.  incoming connection manual Wait for an ATA command before answering an incoming network connection.  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.  blow blistory Displays the current configuration.  blow history Displays the last 20 commands entered during the current CLI session.  blows 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 commands  clrscrn Clears the screen.  Celars the screen.  Celars the screen.  Sets the CONNECT string used in modem emulation.  - string> = connect string.  default incoming connection	error unknown commands enable	Returns an error upon unknown AT commands.
incoming connection disabled  incoming connection manual  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  Response type numeric  Uses numeric type responses.  Response type text  Uses text type responses.  Show  Displays the current configuration.  Show status  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 commands  Clears the screen.  Connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connection  Default disables incoming network connections.</string></text>	exit	Returns to the tunnel level.
incoming connection manual  Wait for an ATA command before answering an incoming network connection.  Removes optional CONNECT string information for modem emulation.  Response type numeric  Asserts tunnel modem status with current configured values.  It is stated to the form of the modem status with current configured values.  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 commands  Clears the screen.  Connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  Default disables incoming network connections.</string></text>	incoming connection automatic	Automatically answer incoming network connections.
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 commands  clrscrn  Clears the screen.  Connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connection  Default disables incoming network connections.</string></text>	incoming connection disabled	Disable incoming network connections.
dem emulation.  reassert  Asserts tunnel modem status with current configured values.  response type numeric  Uses numeric type responses.  response type text  Uses text type responses.  bipplays the current configuration.  bipplays the last 20 commands entered during the current CLI session.  bipplays 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 commands  clrscrn  Clears the screen.  Connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connection  Default disables incoming network connections.</string></text>	incoming connection manual	
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 commands  clrscrn Clears the screen.  Connect string <text> Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connection Default disables incoming network connections.</string></text>	no connect string	Removes optional CONNECT string information for modem emulation.
response type text  show  Displays the current configuration.  Displays the last 20 commands entered during the current CLI session.  Show status  Displays tunnel modem status.  Displays tunnel modem Response Codes.  Verbose response disable  Does not send Modem Response Codes out on the Serial Line.  Verbose response enable  Sends Modem Response Codes out on the Serial Line.  Vertice  Stores the current configuration in permanent memory.  The connect string < text>  Clears the screen.  Connect string < text>  Sets the CONNECT string used in modem emulation. <a href="mailto:string">&lt; string</a> = connect string.  Default disables incoming network connections.	reassert	
show bistory 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 commands  Clears the screen.  Connect string <text> Sets the CONNECT string used in modem emulation.  <string> = connect string.  Default disables incoming network connections.</string></text>	response type numeric	Uses numeric type responses.
show history  Displays the last 20 commands entered during the current CLI session.  Show status  Displays tunnel modem status.  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 commands  clrscrn  Clears the screen.  Connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  Default disables incoming network connections.</string></text>	response type text	Uses text type responses.
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 commands  clrscrn  Clears the screen.  Connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connection  Default disables incoming network connections.</string></text>	show	Displays the current configuration.
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 commands       Clears the screen.         clrscrn       Clears the screen.         connect string <text>       Sets the CONNECT string used in modem emulation.         <string> = connect string.         default incoming connection       Default disables incoming network connections.</string></text>	show history	
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 commands       Clears the screen.         clrscrn       Clears the screen.         connect string <text>       Sets the CONNECT string used in modem emulation.         <string> = connect string.         default incoming connection       Default disables incoming network connections.</string></text>	show status	Displays tunnel modem status.
write  Stores the current configuration in permanent memory.  modem (tunnel-modem:3) level commands  clrscrn  Clears the screen.  connect string <text>  Sets the CONNECT string used in modem emulation.  <string> = connect string.  Default disables incoming network connections.</string></text>	verbose response disable	Does not send Modem Response Codes.
modem (tunnel-modem:3) level commands  clrscrn Clears the screen.  connect string <text> Sets the CONNECT string used in modem emulation.  <string> = connect string.  default incoming connection Default disables incoming network connections.</string></text>	verbose response enable	Sends Modem Response Codes out on the Serial Line.
clrscrn       Clears the screen.         connect string <text>       Sets the CONNECT string used in modem emulation.         <string> = connect string.         default incoming connection       Default disables incoming network connections.</string></text>	write	Stores the current configuration in permanent memory.
connect string <text> Sets the CONNECT string used in modem emulation. <string> = connect string.  default incoming connection  Default disables incoming network connections.</string></text>	modem (tunnel-modem:3) level commands	
<pre></pre>	clrscrn	Clears the screen.
	connect string <text></text>	
default response type Default uses text type responses.	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: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 mo-
	dem emulation.
reassert	Asserts tunnel modem status with current configured val-
	ues.
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 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.

write seriouse response enable Sends Modern Response Codes out on the Serial Line. write sacking (tunnel-packing:16) level commands classed in the series of	verbose response disable	Does not send Modem Response Codes.
Stores the current configuration in permanent memory.    Clears the screen.	<u> </u>	· ·
Clears the screen.  Clears the screen.  Clears the screen.  Clears the screen.  Clears the send character for packing mode.  default send character  Removes the send character for packing mode.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  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.  Disables 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 hax.  A control character has the form *control>C.  A decimal value character has the form control>C.  A decimal value character has the form 0xFF.  Displays the current configuration.  Show show history  Displays the last 20 commands entered during the current CLL session.  Sets the threshold (byte count). If the queued data reachest his threshold then the data will be sent.  *cytes> = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  *trailing character *control>  Sets the trailing character for packing mode.  The character may be input as text, control, decimal, or hox.  A control character has the form *control>C.  A decimal value, in milliseconds.  *trailing character has the form w99.  A hex value character has the form oxFF.  Stess the trailing character for packing mode.  The character has the form oxFF.  Stess the current configuration in permanent memory.  *A control character has the form oxFF.  Stess the current configuration in permanent memory.  *A control character has the form oxFF.  *Steps the current configuration in permanent mem	·	·
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.  Restores the default packing mode timeout.  Returns to the tunnel level.  Returns to the tunnel level.  Removes the trailing character for packing mode.  Disables packing. Data is sent to the network when received.  Disables 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 for packing mode.  The character for packing mode.  The character has the form control>C. A decimal value character has the form (soft).  Show  Displays the last 20 commands entered during the current configuration.  Displays the last 20 commands entered during the current current configuration.  Displays the last 20 commands entered during the current current current configuration.  Sets the threshold (byte count). If the queued data reaches this threshold.  Sets the threshold (byte count). If the queued data reaches this threshold.  Sets the threshold (byte count). If the queued data reaches this threshold.  Sets the threshold (byte count). If the queued data reaches this threshold.  Sets the trailing character for packing mode.  The character has the form (soft).  A control character has the form (soft).  Sets the trailing character for packing mode.  The character has the form (soft).  A control character has the form (soft).  A control character has the form (soft).  Sets the trailing character for packing mode.  The character has the form (soft).  Sets the trailing character has the form (soft).  A control character has the form (soft).  Sets the tireuch valu		I
default threshold default threshold Restores the default threshold. default threshold Restores the default threshold. default threshold Restores the default threshold. default timeout Restores the default threshold. default default timeout. Restores the default threshold. default defau		
default threshold  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.  Disables packing mode disable  packing mode send character  Disables 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).  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 (sont for yo.)  A hex value character has the form (sont for yo.)  A hex value character has the form (sont for yo.)  A hex value character has the form (sont for yo.)  Sets the threshold (byte count). If the queued data reaches this threshold  then the data will be sent.  Solts the imeout value for packing mode in milliseconds.  A control character rhas the form (sont for yo.)  Sets the timeout value for packing mode in milliseconds.  A control character has the form (sont for yo.)  Sets the timeout value for packing mode in milliseconds.  A control character has the form (sont for yo.)  Sets the timeout value for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A control character has the form (sont for yo.)  A c</control>		
default timeout exit Returns to the tunnel level.		
Returns to the tunnel level.  no trailing character  Removes the trailing character for packing mode.  Disables packing. Data is sent to the network when received.  Disables 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 <control>C. A decimal value character has the form \text{Northol}.  Show  Displays the last 20 commands entered during the current CLL session.  Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.  - cytes&gt; = number of bytes in the threshold.  Sets the timeout value for packing mode.  The character has the form <control>C. A decimal value character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form control&gt;C. A decimal value character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form \text{Northol}.  Sets the trailing character for packing mode.  The character has the form \text{Northol}.  A control character has the form \text{Northol}.  A decimal value character has the form \text{Northol}.  A control character has the form \text{Northol}.  Sets the current configuration in permanent memory.  Packing (tunnel-packing:15) level commands  Clears the screen.  default packing mode  default packing mode  default threshold  default threshold  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.</control></control>		
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).  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 <control>C. A decimal value character has the form \(0.000)  A hex value character has the form \(0.000)  Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.  <!--</td--><td></td><td></td></control></control></control>		
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).  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 VsF.  Show  Displays the current configuration.  Displays the last 20 commands entered during the current cL1 session.  Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.                 timeout <milliseconds>  Sets the timeout value for packing mode in milliseconds.  A control character may be input as text, control, decimal, or hex.    Sets the timeout value for packing mode in milliseconds.  **Tilliseconds&gt;** It immout value, in milliseconds.  **Tilliseconds&gt;** It immout value, in milliseconds.  **Tilliseconds&gt;** It immout value, in milliseconds.  **A control character may be input as text, control, decimal, or hex.  A control character has the form ventrol&gt;C.  A decimal value character has the form oxFF.  Stores the current configuration in permanent memory.  **Packing (tunnel-packing:15) level commands**  Clears the screen.  default packing mode  Sets to default packing mode, which is "Disable"  default packing mode  Restores the default packing mode timeout.  Restores the default packing mode timeout.  Restores the default packing mode timeout.  Restores the default packing mode timeout.</milliseconds></control></control>		
ceived.  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 control>C. A decimal value character has the form OXFF.  Show  Show bistory  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 bytes> = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  trailing character <control>  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&gt;C. A decimal value character has the form V99. A hex value character has the form CXFF.  Stores the current configuration in permanent memory.  Packing (unnel-packing:15) level commands  cirsorn  Clears the screen.  default packing mode  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default packing mode timeout.  Restores the default packing mode timeout.  Restores the default packing mode timeout.</control>		
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 <cntrol>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 (byte count). If the queued data reaches this threshold then the data will be sent. <a href="https://doi.org/10.1006/j.com/pack-nulliseconds">https://doi.org/10.1006/j.com/pack-nulliseconds</a>  Sets the timeout value for packing mode in milliseconds.  Itrailing 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 <cntrol>C. A decimal value character has the form </cntrol>C. A decimal value character has the form 0xFF.  write  Stores the current configuration in permanent memory.  packing (tunnel-packing:15) level commands cirscrn  Clears the screen.  Clears the screen.  Clears the screen.  default packing mode, which is "Disable"  default send character  Removes the send character for packing mode.  default threshold  default threshold  default threshold  default threshold  Restores the default packing mode timeout.  Restores the default packing mode timeout.  Restores the default packing mode timeout.</control></cntrol></control>	packing mode disable	
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 \(\mathbb{V}\)99. A hex value character has the form \(\mathbb{V}\)99. A hex value character has the form \(\mathbb{V}\)95.  show  Show bistory  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.                   timeout <milliseconds>  Sets the timeout value for packing mode in milliseconds.    </milliseconds></control></control>	packing mode send character	upon receiving the
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 \( \text{ 99}.\) A hex value character has the form \( \text{ 99}.\) A hex value character has the form \( \text{ 99}.\) Show  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 (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold.  Sets the timeout value for packing mode in milliseconds.  A control character has the form \( \text{ 90} \) and the packing mode. The character may be input as text, control, decimal, or hex.  A control character has the form \( \text{ 99}.\) and hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) and hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) a hex value character has the form \( \text{ 99}.\) and hex value character has the form \( </control>	packing mode timeout	after a specified
Displays the last 20 commands entered during the current CLI session.  Sets the threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold then the data will be sent.	send character <control></control>	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.</control>
threshold threshold threshold threshold threshold threshold threshold (byte count). If the queued data reaches this threshold (bytes) in the threshold.  Sets the threshold then the data will be sent.        timeout <milliseconds>    Sets the timeout value for packing mode in milliseconds.   <br< td=""><td>show</td><td>Displays the current configuration.</td></br<></milliseconds>	show	Displays the current configuration.
es this threshold then the data will be sent.     timeout <milliseconds>     Sets the timeout value for packing mode in milliseconds.   <milliseconds> = timeout value, in 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 \moxFF.    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.</control></milliseconds></milliseconds></milliseconds>	show history	Displays the last 20 commands entered during the current CLI session.
Amilliseconds> = 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 <a href="#">Control</a> A decimal value character has the form <a href="#">(Nec of the control</a> A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character has the form <a href="#">(Nec of the control</a> C. A decimal value character for packing mode. The control value has the form <a href="#">(Nec of the control value has the form <a href="#">(Nec of the control value has the form <a href="#">(Nec of the control value has the form <a href="#">(Nec of the control value has the form <a href="#">(Nec of the control value has the form <a character="" default="" disable"="" exit="" for="" href="&lt;/td&gt;&lt;td&gt;threshold &lt;br/&gt; threshold &lt;br/&gt;&lt;/td&gt;&lt;td&gt;then the data will be sent.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;The character may be input as text, control, decimal, or hex.  A control character has the form &lt;control&gt;C.  A decimal value character has the form \99.  A hex value character has the form 0xFF.  write  Stores the current configuration in permanent memory.  packing (tunnel-packing:15) level commands  clrscrn  Clears the screen.  default packing mode  default packing mode, which is " level.="" mode="" mode.="" mode.<="" packing="" removes="" restores="" returns="" send="" td="" the="" threshold="" timeout="" timeout.="" to="" trailing="" tunnel=""><td>timeout <milliseconds></milliseconds></td><td></td></a></a></a></a></a></a>	timeout <milliseconds></milliseconds>	
clrscrn Clears the screen.  default packing mode default send character Removes the send character for packing mode.  default threshold Restores the default threshold.  default timeout exit Returns to the tunnel level.  Removes the screen.  Removes the screen.  Removes the send character for packing mode.  Restores the default threshold.  Returns to the tunnel level.  Removes the trailing character for packing mode.	trailing character < control>	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.</control>
clrscrn  default packing mode  default packing mode  default send character  default threshold  default timeout  exit  no trailing character  Clears the screen.  Clears the screen.  Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.	write	Stores the current configuration in permanent memory.
default packing mode  default packing mode, which is "Disable"  default send character  default threshold  default timeout  exit  no trailing character  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.	packing (tunnel-packing:15) level comman	ds
default send character  default threshold  default timeout  exit  no trailing character  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.	clrscrn	Clears the screen.
default threshold  default timeout  exit  no trailing character  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.	default packing mode	Sets to default packing mode, which is "Disable"
default timeout  exit  Restores the default packing mode timeout.  Returns to the tunnel level.  Removes the trailing character for packing mode.	default send character	Removes the send character for packing mode.
exit Returns to the tunnel level.  no trailing character Removes the trailing character for packing mode.	default threshold	Restores the default threshold.
no trailing character Removes the trailing character for packing mode.	default timeout	Restores the default packing mode timeout.
	exit	Returns to the tunnel level.
packing mode disable Disables packing. Data is sent to the network when re-	no trailing character	Removes the trailing character for packing mode.
	packing mode disable	Disables packing. Data is sent to the network when re-

	ceived.
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.         Sets the threshold (byte count). If the queued data reaches this threshold (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:14) level commands	
packing (tunnel-packing:14) level commands clrscrn	Clears the screen.
	Clears the screen.  Sets to default packing mode, which is "Disable"
clrscrn	
clrscrn default packing mode	Sets to default packing mode, which is "Disable"
clrscrn default packing mode default send character	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.
clrscrn default packing mode default send character default threshold	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.
clrscrn default packing mode default send character default threshold default timeout	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.
clrscrn default packing mode default send character default threshold default timeout exit	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.
clrscrn default packing mode default send character default threshold default timeout exit no trailing character	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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 re-
clrscrn default packing mode default send character default threshold default timeout exit no trailing character packing mode disable	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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
clrscrn default packing mode default send character default threshold default timeout exit no trailing character packing mode disable packing mode send character	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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
clrscrn default packing mode default send character default threshold default timeout exit no trailing character packing mode disable  packing mode send character  packing mode timeout	Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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 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.</control>

	CLI session.
threshold <bytes></bytes>	Sets the threshold (byte count). If the queued data reach-
	es this threshold
	then the data will be sent.
	<pre><bytes> = number of bytes in the threshold.</bytes></pre>
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.</control>
	A decimal value character has the form \99.
	A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:13) 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 re-
packing mode disable	ceived.
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
packing mode timeout	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.</control>
	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  threshold  	Sets the threshold (byte count). If the queued data reach-
	es this threshold
	then the data will be sent.  <b< td=""></b<>
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds.
unicout (Illinocoolido)	sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character <control></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.</control>
	A decimal value character has the form \99.
	A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:12) 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.     - Note that 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></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 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 re-
packing mode disable	ceived.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).

	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></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 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.  

Armilliseconds> = timeout value, in milliseconds.		
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 WPP.  A hex value character has the form WPP.  Stores the current configuration in permanent memory.  Packing (tunnel-packing:9) level commands  cirsorn  Clears the screen.  Clears the screen.  default packing mode  Sets to default packing mode, which is "Disable" default threshold.  Restores the default threshold.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.  Returns to the tunnel level.  Removes the trailing character for packing mode.  Disables packing. Data is sent to the network when received.  Packing mode disable  Disables 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 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 9. A hex value character has the form 9. A hex value character has the form (by.)  A control character has the form (by.)  Sets the threshold then the data will be sent.  chytes>  Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.  chytes>  It her active that the threshold.  Sets the timeout value for packing mode in milliseconds.  Sets the timeout value for packing mode in milliseconds.  Sets the timeout value for packing mode in milliseconds.  Sets the timeout value for packing mode in milliseconds.  Sets the timeout value for packing mode.  The character has the form WPF.  Stores the current configuration in permanent memory.  Packing (tunnel-packing:8) level commands  Clears the screen.  Sets t	timeout <milliseconds></milliseconds>	
cirsorn  Clears the screen.  Clears the screen.  default packing mode  default packing mode  default send character  Removes the send character for packing mode.  Restores the 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.  Packing mode disable  Disables 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).  Send character <a href="#">Sets the send character for packing mode.</a> Packing mode timeout  Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).  Send character <a href="#">Sets the send character for packing mode.</a> The character may be input as text, control, decimal, or hex.  A control character has the form yea.  A control character has the form yea.  A control character has the form oxFF.  Displays the current configuration.  Show history  Displays the current configuration.  Sets the threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count) and the sent.  -bytes> = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  crilliseconds> = timeout value for packing mode in milliseconds.  Trailing character <a href="#">Control character has the form control&gt;C.</a> A control character has the form <a href="#">Control character has the form sent.  -bytes&gt; = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  -crilliseconds&gt; = timeout value for packing mode.  The character has the form <a href="#">Control character has the form yea.  - A control charac</a></a>	trailing character < control>	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.</control>
cirsorn  Clears the screen.  Clears the screen.  default packing mode  default packing mode  default send character  Removes the send character for packing mode.  Restores the 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.  Packing mode disable  Disables 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).  Send character <a href="#">Sets the send character for packing mode.</a> Packing mode timeout  Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).  Send character <a href="#">Sets the send character for packing mode.</a> The character may be input as text, control, decimal, or hex.  A control character has the form yea.  A control character has the form yea.  A control character has the form oxFF.  Displays the current configuration.  Show history  Displays the current configuration.  Sets the threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count) and the sent.  -bytes> = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  crilliseconds> = timeout value for packing mode in milliseconds.  Trailing character <a href="#">Control character has the form control&gt;C.</a> A control character has the form <a href="#">Control character has the form sent.  -bytes&gt; = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  -crilliseconds&gt; = timeout value for packing mode.  The character has the form <a href="#">Control character has the form yea.  - A control charac</a></a>	write	Stores the current configuration in permanent memory.
Clears the screen.	packing (tunnel-packing:9) level commands	
default send character default threshold Restores the default threshold. default timeout Restores the default packing mode timeout. exit Returns to the tunnel level. Removes the trailing character for packing mode. Disables packing. Data is sent to the network when received.  packing mode disable Disables 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 <a href="control">configured send character on the line (serial port)</a> .  Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \(\frac{1}{2}\) A hex value character has the form \(\frac{1}{2}\) A hex value character has the form \(\frac{1}{2}\) Sets the trieshold (byte count). If the queued data reaches this threshold then the data will be sent. <a href="control">control</a> Sets the timeout value for packing mode in milliseconds.  trailing character <a href="control">control</a> Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \(\frac{1}{2}\) Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <a href="control">control</a> Sets the timeout value for packing mode in milliseconds.  trailing character <a href="control">control</a> Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form \(\frac{1}{2}\) A hex value character has the form \(\frac{1}{2}\) A		Clears the screen.
default threshold default timeout Restores the default packing mode timeout. exit Returns to the tunnel level. Removes the trailing character for packing mode. 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).  sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).  send character <control> 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 on the line (serial port).  Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form (serial port).  Show Displays the current configuration.  Displays the current configuration.  CLI session.  Sets the threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count).  Sets the timeout value for packing mode in milliseconds.  **cmilliseconds&gt;** cmilliseconds&gt;** cmilliseconds** cmilliseconds** cmilliseconds** cmilliseconds** cmilliseconds** cmilliseconds** cmilliseconds** cmilliseconds*</control>	default packing mode	Sets to default packing mode, which is "Disable"
default timeout exit no trailing character 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 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 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 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. clytes> = number of bytes in the threshold.  Sets the timeout value, in milliseconds.  A control character may be input as text, control, decimal, or hex.  A control character may be input as text, control, decimal, or hex.  A control character has the form control>C. A decimal value character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form 0xFF.  Stores the current configuration in permanent memory.  Packing (tunnel-packing:8) level commands  cliscrn Clears the screen.  Clears the screen.  Clears the screen.  Clears the send character for packing mode.	default send character	Removes the send character for packing mode.
Returns to the tunnel level.  Removes the trailing character for packing mode.  Disables packing. Data is sent to the network when received.  Packing mode send character  Packing mode send character  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 \square.  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.  **Trailing character <**Control**  Sets the timeout value for packing mode in milliseconds.  **Initiage character has the form \square \square \square \text{A control} \square \text{CI session.}  Sets the timeout value, in milliseconds.  **Trailing character <**Control**  **Sets the trailing character for packing mode in milliseconds.  **Trailing character for packing mode.**  The character may be input as text, control, decimal, or hex.  A control character has the form \square \square \text{A control} \square \text	default threshold	Restores the default threshold.
no trailing character  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 the send character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form \(\frac{1}{2}\) A control character has the form \(\frac{1}{2}\) A control character has the form \(\frac{1}{2}\) A hex value character has the form \(\frac{1}{2}\) Fixed the send of the threshold (byte count). If the queued data reachests this threshold \(\frac{1}{2}\) the sent.  Sets the timeout \(\frac{1}{2}\) milliseconds entered during the current CLI session.  Sets the threshold (byte count). If the queued data reachests this threshold then the data will be sent.  Softs the timeout value for packing mode in milliseconds.  A control character has the form \(\frac{1}{2}\) commands entered bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  **The character may be input as text, control, decimal, or hex.  A control character has the form \(\frac{1}{2}\) commands entered during the current configuration in permanent memory.  A control character has the form \(\frac{1}{2}\) commands  **The character	default timeout	Restores the default packing mode timeout.
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).  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 0xFF.  Show  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.   <a 10.2016="" doi.<="" doi.org="" href="https://doi.org/10.1001/j.com/bits/10.1001/j.com&lt;/td&gt;&lt;td&gt;exit&lt;/td&gt;&lt;td&gt;Returns to the tunnel level.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;ceived.  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 &lt;control&gt;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.  threshold &lt;br/&gt; threshold &lt;br/&gt; the data will be sent. &lt;br/&gt;&lt;br/&gt; &lt;br/&gt; &lt;&lt;/td&gt;&lt;td&gt;no trailing character&lt;/td&gt;&lt;td&gt;Removes the trailing character for packing mode.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;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).  send character &lt;control&gt;  Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form &lt;control&gt;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 will be sent. &lt;a href=" https:="" j.com="" td=""><td>packing mode disable</td><td></td></a></control></control>	packing mode disable	
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.  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.         </control>	packing mode send character	upon receiving the
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.  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.                   timeout <milliseconds>  Sets the timeout value for packing mode in milliseconds.   <br< td=""><td>packing mode timeout</td><td>after a specified</td></br<></milliseconds></control>	packing mode timeout	after a specified
bisplays 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. 	send character <control></control>	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.</control>
threshold threshold threshold threshold threshold threshold the threshold then the data will be sent.    timeout <milliseconds>   Sets the timeout value for packing mode in milliseconds.             The character for packing mode. The character may be input as text, control, decimal, or hex.   A control character has the form   A control character has the form 0xFF.     write Stores the current configuration in permanent memory.             Clears the screen.   Sets to default packing mode, which is "Disable"   Removes the send character for packing mode.</milliseconds>	show	Displays the current configuration.
es this threshold then the data will be sent.   <	show history	
<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 0y9. A hex value character has the form 0xFF. write Stores the current configuration in permanent memory. packing (tunnel-packing:8) level commands clrscrn Clears the screen. Gefault packing mode, which is "Disable" Removes the send character for packing mode.</control></control></milliseconds>	threshold bytes>	es this threshold then the data will be sent.
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.  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"  Removes the send character for packing mode.</control>	timeout <milliseconds></milliseconds>	
packing (tunnel-packing:8) level commands  clrscrn  default packing mode  default send character  Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.	trailing character <control></control>	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.</control>
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.	write	Stores the current configuration in permanent memory.
default packing mode Sets to default packing mode, which is "Disable" default send character Removes the send character for packing mode.	packing (tunnel-packing:8) level commands	
default send character Removes the send character for packing mode.	clrscrn	Clears the screen.
	default packing mode	Sets to default packing mode, which is "Disable"
default threshold Restores the default threshold.	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 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.</control>
	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.  
timeout <milliseconds></milliseconds>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds>
trailing character <control></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 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.      - 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.

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 \vert \vert</control>		A control character has the form <control>C.</control>
Stores the current configuration in permanent memory.  Clears the screen.  Clears the screen.  Clears the screen.  Gefault packing mode  Gefault packing mode  default send character  Removes the send character for packing mode.  default threshold  Restores the default threshold.  Restores the default packing mode timeout.  Restores 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 the send character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form (soff).  A decimal value character has the form (soff).  Show  Displays the current configuration.  Displays the current configuration.  Displays the current configuration.  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.  Sets the timeout value for packing mode in milliseconds.  The character has the form control-C.  A decimal value character for packing mode.  The character has the form open one.  The character has the form open open open open open open open open		
Clears the screen.		
Clears the screen.  Clears the screen.  Clears the screen.  Sets to default packing mode, which is "Disable" default packing mode default send character for packing mode.  default tendence the send character for packing mode.  default timeout  Restores the default packing mode timeout.  Restores the default packing mode 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.  packing mode disable  Disables 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 <pre> A control character has the form <pre> Sets he send character has the form <pre> Sets he instead of the send of the se</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>		Stores the current configuration in permanent memory.
default packing mode  default send character  default threshold  default threshold  Restores the default threshold.  Restores the default threshold.  Restores the default threshold.  default timeout  Restores the default threshold.  Restores the default packing mode, which is "Disable"  Restores the default threshold.		
default send character  default threshold  Restores the default threshold.  Restores the default packing mode timeout.  Restores the trailing character for packing mode.  Disables packing. Data is sent to the network when received.  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  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 <a href="#">A control character has the form <a href="#">Configured send character has the form <a href="#">Configured send character for packing mode.</a>  The character may be input as text, control, decimal, or hex.  A control character has the form <a href="#">A control character has the form <a href="#">Control character</a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a>		
default threshold default timeout exit Returns to the tunnel level. Disables packing mode disable Disables packing mode to the network when received. Packing mode send character Packing mode send character  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 or packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <pre>CA</pre> A decimal value character has the form <pre>VFP 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>cbytes&gt;</pre> Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <pre>cbytes = number of bytes in the threshold.</pre> Sets the timeout value for packing mode in milliseconds.  smilliseconds&gt; = timeout value, in milliseconds.  trailing character <pre>control&gt;</pre> Sets the trailing character for packing mode. The character has the form <pre>VFP</pre> A control character has the form <pre>VFP</pre> A control character has the form <pre>VFP</pre> Stores the current configuration in permanent memory. Packing (tunnel-packing:4) level commands clirican Clears the screen.  Clears the screen.  Clears the send character for packing mode. Restores the default threshold.</pre>		
default timeout exit Restores the default packing mode 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 send character  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 vontrol>C. A decimal value character has the form vontrol>C. A decimal value character has the form vontrol because threshold (bytes>  Sets the threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold (byte count).  Sets the timeout value for packing mode in milliseconds.  The character may be input as text, control, decimal, or hex.  Sets the timeout value character has the form vontrol>C. A decimal value character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form vontrol>C. A decimal value character has t		
Returns to the tunnel level.  Removes the trailing character for packing mode.  Disables packing. Data is sent to the network when received.  packing mode send character  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).  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. (byte="" <br="" a="" be="" character="" cli="" count).="" data="" decimal="" fe.="" form="" has="" hex="" if="" out="" queued="" reaches="" sent.="" session.="" sets="" the="" then="" this="" threshold="" v99.="" value="" will=""></control-c.>   Sets the timeout value for packing mode in milliseconds.  A control character for packing mode in milliseconds.  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. (tunnel-packing="" 4)="" <control-c.="" a="" as="" be="" character="" clears="" commands="" configuration="" control="" control,="" current="" decimal="" decimal,="" decking="" for="" form="" has="" hex.="" in="" input="" level="" may="" memory.="" mode.="" mode.<="" or="" packing="" permanent="" removes="" screen.="" send="" set.="" stores="" td="" text,="" the="" to="" value=""><td></td><td></td></control-c.>		
no trailing character  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 acking 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>A control</pre> Show  Show  Displays the last 20 commands entered during the current CLI session.  Sets the threshold (byte count). If the queued data reachesth is threshold then the data will be sent.  chytes> sets the most value for packing mode in milliseconds.  **Trailing character <pre>control&gt;</pre> Sets the trailing character for packing mode.  The character may be input as text, control, decimal, or hex.  Sets the timeout value for packing mode in milliseconds.  **Trailing character <pre>control&gt;</pre> 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>CA</pre> A decimal value character has the form <pre>control&gt;CA</pre> A decimal value character has the form <pre>OxFF</pre> Stores the current configuration in permanent memory.  **Packing (tunnol-packing:4) level commands  Clears the screen.  Clears the screen.  Clears the screen.  default packing mode, which is "Disable" Removes the send character for packing mode.  Removes the send character for packing mode.  Restores the default threshold.		
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 control>C.  A decimal value character has the form QSF.  Show  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.  -bytes> = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.  -trailing character <control>  Sets the timeout value for packing mode in milliseconds.  -trailing character ray be input as text, control, decimal, or hex.  A control character has the form control&gt;C.  A decimal value character for packing mode.  The character may be input as text, control, decimal, or hex.  A control character has the form control&gt;C.  A decimal value character has the form yo9.  A hex value character has the form woFF.  Stores the current configuration in permanent memory.  Packing (tunnel-packing:4) level commands of the current configuration in permanent memory.  Clears the screen.  Gefault packing mode, which is *Disable*  default send character for packing mode.  Restores the default threshold.</control>		
ceived.  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).  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 \(0.9\). A hex value character has the form \(0.9\). A hex value character has the form \(0.9\). A hex value character has the form \(0.9\). Sets the threshold (byte count). If the queued data reaches this threshold   thereshold   show Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.   chytes&gt; = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds.   chilliseconds&gt; = timeout value, in milliseconds.   chilliseconds = timeout value, in milliseconds.   A control character has the form   A control character has the form \(0.9\). A hex value character h</control></control>		
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 \mostype{\text{VF}}.  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. <a character="" default="" disable"="" for="" href="https://doi.org/10.1001/j.com/&lt;/td&gt;&lt;td&gt;packing mode disable&lt;/td&gt;&lt;td&gt;ceived.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;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 &lt;pre&gt;control&lt;/pre&gt; A decimal value character has the form 099. A hex value character has the form 0xFF.  Show  Displays the current configuration.  Displays the last 20 commands entered during the current CL1 session.  Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. &lt;pre&gt;cytes&gt; = number of bytes in the threshold.&lt;/pre&gt;  Sets the timeout &lt;milliseconds&gt;  strailing character &lt;control&gt;  Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form &lt;control&gt;C. A decimal value character has the form &lt;control&gt;C. C default packing (tunnel-packing:4) level commands Clrscrn Clears the screen.  default packing mode default packing mode, which is " mode.="" packing="" removes="" restores="" send="" td="" the="" threshold="" threshold.<=""><td>packing mode send character</td><td>upon receiving the</td></a></control>	packing mode send character	upon receiving the
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.  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 (byte count). If the queued data reaches this threshold then the data will be sent. &lt;</control>	packing mode timeout	after a specified
Displays the last 20 commands entered during the current CLI session.  Sets the threshold (byte count). If the queued data reaches this threshold (byte count). If the queued data reaches this threshold will be sent.   	send character <control></control>	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.</control>
threshold threshold threshold threshold threshold the threshold (byte count). If the queued data reaches this threshold then the data will be sent.        timeout <milliseconds>    Sets the timeout value for packing mode in milliseconds.   <milliseconds> = timeout value, in milliseconds.   <mi>A control character has the form control&gt;C. A decimal value character has the form 0xFF.   <mi>A control character has the form 0xFF.   <mi>Stores the current configuration in permanent memory.   <mi>Packing (tunnel-packing:4) level commands  <mi>Clears the screen. </mi>   Clears the screen.   default packing mode   default packing mode, which is "Disable"   Removes the send character for packing mode.   default threshold   Restores the default threshold.</mi></mi></mi></mi></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds></milliseconds>	show	Displays the current configuration.
es this threshold then the data will be sent.	show history	
<a character="" default="" disable"="" for="" href="mailto:kma&lt;/td&gt;&lt;td&gt;threshold &lt;br/&gt; bytes&gt;&lt;/td&gt;&lt;td&gt;es this threshold then the data will be sent.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;The character may be input as text, control, decimal, or hex.  A control character has the form &lt;control&gt;C.  A decimal value character has the form \99.  A hex value character has the form 0xFF.  Stores the current configuration in permanent memory.  packing (tunnel-packing:4) level commands  clrscrn  Clears the screen.  default packing mode  default send character  Removes the send character for packing mode.  Restores the default threshold.&lt;/td&gt;&lt;td&gt;timeout &lt;milliseconds&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;clrscrn Clears the screen.  default packing mode default send character  default threshold  Restores the default threshold.&lt;/td&gt;&lt;td&gt;trailing character &lt;control&gt;&lt;/td&gt;&lt;td&gt;The character may be input as text, control, decimal, or hex. A control character has the form &lt;control&gt;C. A decimal value character has the form \99.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;clrscrn  Clears the screen.  default packing mode  Sets to default packing mode, which is " mode.="" packing="" removes="" restores="" send="" td="" the="" threshold="" threshold.<=""><td>write</td><td>Stores the current configuration in permanent memory.</td></a>	write	Stores the current configuration in permanent memory.
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:4) level commands	
default send character  Removes the send character for packing mode.  Restores the default threshold.	clrscrn	Clears the screen.
default threshold Restores the default threshold.	default packing mode	Sets to default packing mode, which is "Disable"
	default send character	Removes the send character for packing mode.
The same of the sa	default threshold	Restores the default threshold.
default timeout   Restores the default packing mode timeout.	default timeout	Restores the default packing mode timeout.
	exit	
no trailing character Removes the trailing character for packing mode.	no trailing character	Removes the trailing character for packing mode.
packing mode disable  Disables packing. Data is sent to the network when re-		

	ceived.
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.
write packing (tunnel-packing:3) level commands	Stores the current configuration in permanent memory.
12	Stores the current configuration in permanent memory.  Clears the screen.
packing (tunnel-packing:3) level commands	
packing (tunnel-packing:3) level commands clrscrn	Clears the screen.
packing (tunnel-packing:3) level commands clrscrn default packing mode	Clears the screen.  Sets to default packing mode, which is "Disable"
packing (tunnel-packing:3) level commands clrscrn default packing mode default send character	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.
packing (tunnel-packing:3) level commands clrscrn default packing mode default send character default threshold	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.
packing (tunnel-packing:3) level commands clrscrn default packing mode default send character default threshold default timeout	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.
packing (tunnel-packing:3) level commands clrscrn default packing mode default send character default threshold default timeout exit	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  Restores the default packing mode timeout.  Returns to the tunnel level.
packing (tunnel-packing:3) level commands clrscrn default packing mode default send character default threshold default timeout exit no trailing character	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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 re-
packing (tunnel-packing:3) level commands  clrscrn  default packing mode  default send character  default threshold  default timeout  exit  no trailing character  packing mode disable	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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
packing (tunnel-packing:3) level commands  clrscrn  default packing mode  default send character  default threshold  default timeout  exit  no trailing character  packing mode disable  packing mode send character	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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
packing (tunnel-packing:3) level commands  clrscrn  default packing mode  default send character  default threshold  default timeout  exit  no trailing character  packing mode disable  packing mode send character  packing mode timeout	Clears the screen.  Sets to default packing mode, which is "Disable"  Removes the send character for packing mode.  Restores the default threshold.  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 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.</control>

	CLI session.
threshold threshold ithresho	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.
timeout <milliseconds></milliseconds>	<pre><bytes> = number of bytes in the threshold.  Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.</milliseconds></bytes></pre>
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 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 <td>Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent.             - bytes&gt; = number of bytes in the threshold.</br></td>	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 commands	peteres the surrent comiguration in permanent memory.

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.      - 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></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 command	s
cirscrn	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	a password.  Shows the current configuration.

	CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:	15) 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:	14) 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:	13) 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
write	CLI session.  Stores the current configuration in permanent memory.
password (tunnel-accept-password:	_
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 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:	10) 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:9) level command:	S
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:8) level command:	5
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:7) level command	S
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:6) level commands	2 ,
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	
also assa	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
exit	Exits to the next higher level.  Removes the password so connections will be accepted
exit no password	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
exit no password  password <text></text>	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
exit no password password <text> prompt disable</text>	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
exit no password  password <text>  prompt disable  prompt enable</text>	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.
exit no password  password <text>  prompt disable  prompt enable  show show history  write</text>	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.
exit no password  password <text>  prompt disable  prompt enable  show show history</text>	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.
exit no password  password <text>  prompt disable  prompt enable  show show history  write</text>	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.
exit  no password  password <text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:4) level commands</text>	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.
exit  no password  password <text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:4) level commands clrscrn</text>	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.
exit  no password  password < text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:4) level commands clrscrn exit	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.  Clears the screen.  Exits to the next higher level.  Removes the password so connections will be accepted
exit  no password  password <text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:4) level commands clrscrn exit no password</text>	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.  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

	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 command:	
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:2) level commands	
clrscrn	Clears the screen.
lexit	Exits to the next higher level.
	-
no password	Removes the password so connections will be accepted unchallenged.
	Removes the password so connections will be accepted
no password	Removes the password so connections will be accepted unchallenged.  Sets the password required on the network side of the tunnel to begin
no password  password <text></text>	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
no password  password <text>  prompt disable</text>	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
no password  password <text>  prompt disable  prompt enable</text>	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.
no password  password <text>  prompt disable  prompt enable  show show history  write</text>	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.
no password  password <text>  prompt disable  prompt enable  show show history</text>	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.
no password  password <text>  prompt disable  prompt enable  show show history  write</text>	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.
no password  password <text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:1) level command:</text>	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.  Clears the screen.  Exits to the next higher level.
no password  password <text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:1) level commands clrscrn</text>	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.  Clears the screen.  Exits to the next higher level.  Removes the password so connections will be accepted unchallenged.
no password  password <text>  prompt disable  prompt enable  show show history  write  password (tunnel-accept-password:1) level commands clrscrn exit</text>	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.  Clears the screen.  Exits to the next higher level.  Removes the password so connections will be accepted

	I
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.
query port (config-query_port) level commands	
clear counters	Zeros Query Port counters
clrscrn	Clears the screen.
exit	Returns to the config level.
no clear counters	Unzeros Query Port counters
show	Displays statistics and information about the query port.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables response to 77FE requests.
state enable	Permits response to 77FE requests.
write	Stores the current configuration in permanent memory.
root level commands	
clrscrn	Clears the screen.
enable	Enters the enable level.
exit	Exit from the system
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
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.

rtc (config-rtc) level commands	
clock set <time(hh:mm:ss)> <day (1-31)=""> <month text=""></month></day></time(hh:mm:ss)>	Sets the system clock.
<pre></pre> <pre><pre><pre><pre><pre></pre><pre></pre><pre></pre><pre><pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pr< td=""><td>deta the system dock.</td></pr<></pre></pre></pre></pre></pre></pre>	deta the system dock.
clock timezone	Shows possible time zone names.
clock timezone <time zone=""></time>	Sets the timezone to be displayed. Use "clock timezone" to show choices.
clrscrn	Clears the screen.
default clock timezone	Restores the default timezone, which is UTC.
exit	Exits to the configuration level.
show	Displays the system clock.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:16) 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:15) 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:14) 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.

dr unasserted exit Returns to the tunnel level.  Show  Displays the last 20 commands entered during the current CLI session.  Write Stores the current configuration in permanent memory.  Serial (tunnel-serial-13) level commands  clescen Clears the screen.  default dr Restores default DTR control, 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.  by the current configuration in permanent memory.  Serial (tunnel-serial-12) level commands  clrscm Classision.  Clears the screen.  default dr Restores default DTR control, asserted while connected.  Asserts DTR regardless of any connections and the current configuration in permanent memory.  Serial (tunnel-serial-12) level commands  clrscm Classis the screen.  default dr Restores default DTR control, 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 be match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  exit Returns to the tunnel level.  show  Displays the last 20 commands entered during the current CLI session.  Write Scried (tunnel-serial-11) level commands  Clears the screen.  Clears the screen connect or accept mode tunnel connection is active.  Asserts DTR to match remote DSR when connected via Telnet.  The tunnel serial-11 level commands  Clears the screen connect or accept mode tunnel connected with tunnel level.  Stores the current configuration in perma	dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
show history  Displays the last 20 commands entered during the current colliguration.  Show history  CLI session.  Write  Stores the current configuration in permanent memory.  Serial (tunnel-serial:13) level commands  clicars memory.  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 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.  Displays the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands  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 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 capacities of any connections.  dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Scrial (tunnel-serial:12) level commands  clears the screen.  default dtr  Asserts DTR capacitiess of any connections.  dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  Stores the current configuration in permanent memory.  Scrial (tunnel-serial:11) level commands  clears the screen.  Asserts DTR control, asserted while connected.  Asserts DTR to match remote DSR when connected.  Asserts DTR to match remote DSR when connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted  dtr continuously asserted  Does not assert DTR.  Asserts DTR to match remote DSR when connected.  Asserts DTR whenever a connect or	dtr unasserted	Does not assert DTR.
show history  Displays the last 20 commands entered during the current CLI session.  Write  Stores the current configuration in permanent memory.  Sorial (tunnel-sorial:13) lovel commands  cirscm  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 unasserted  Does not assert DTR.  Sorial (tunnel-sorial:12) lovel commands  cirscm  Clears the screen.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr unasserted  Does not assert DTR.  Sorial (tunnel-sorial:12) lovel commands  cirscm  Clears the screen.  Clears the screen.  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted  Does not assert DTR.  Returns to the tunnel level.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr unasserted  Does not assert DTR.  Returns to the tunnel level.  Show  Displays the last 20 commands entered during the current configuration in permanent memory.  Asserts DTR regardless of any connections.  dtr truport  Asserts DTR regardless of any connections.  dtr unasserted  Does not assert DTR.  Returns to the tunnel level.  Show  Displays the last 20 commands entered during the current configuration in permanent memory.  Sorial (tunnel-sorial:11) level commands  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR whenever a connect or accept mode	exit	Returns to the tunnel level.
CLI session.  Stores the current configuration in permanent memory.  Serial (tunnel-serial:13) 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.  blisplays the last 20 commands entered during the current CLI session.  write  Stores the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands  clrscrn  Clears the screen.  Gefault 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 unasserted  Asserts DTR memore DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  exit  Returns to the tunnel level.  show  Displays the last 20 commands entered during the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands  dtr truport  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr unasserted  Asserts DTR to match remote DSR when connected via Telnet.  exit  Returns to the tunnel level.  Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR to match remote DSR when connected via Telnet.  dtr continuously asserted  Asserts DTR repardless of any connections.  dtr truport  Asserts DTR repardless of any connections.  dtr unasserted while connected  Asserts DTR repardless of any connections.  dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Asserts DTR to match remote DSR when connected via Telnet.	show	Displays the current configuration.
cirsorn  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 to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  show bistory  Displays the last 20 commands entered during the current CLI session.  Sarial (tunnel-serial:12) level commands  cirsorn  Asserts DTR connected via Telnet.  Clears the screen.  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR connected is active.  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Current configuration in permanent memory.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Current continuously asserted  Asserts DTR regardless of any connections.  Asserts DTR omatch remote DSR when connected via Telnet.  Current configuration.  Displays the last 20 commands entered during the current connection is active.  Current connection is active.  Current connection is active.  Current configuration.  Does not assert DTR.  Returns to the tunnel level.  Stores the current configuration.  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration.  Displays the last 20 commands entered during the current CLI session.  Cicars the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Clears the screen.  Des not assert DTR.  Restores default DTR control, asserted while connected via Telnet.  Clears the screen.  Displays the last 20 commands entered during the current configuration in permanent mem	show history	
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 Teinet. dtr unasserted Does not assert DTR. exit Returns to the tunnel level. show Displays the current configuration. showhistory Displays the last 20 commands entered during the current CLI session. write Stores the current configuration in permanent memory. Serial (tunnel-serial:12) level commands clirsorn 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 dtr truport Asserts DTR or match remote DSR when connected via Teinet. dtr unasserted Does not assert DTR. exit Returns to the tunnel level. show Displays the current configuration in permanent memory. Serial (tunnel-serial:11) level commands clirsorn Clears the screen. default dtr description asserted Asserts DTR or match remote DSR when connected via Teinet. dtr unasserted Does not assert DTR. exit Returns to the tunnel level. show Displays the current configuration in permanent memory. Serial (tunnel-serial:11) level commands clirsorn 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 whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted Asserts DTR or match remote DSR when connected via Teinet.  dtr unasserted while connected Asserts DTR or match remote DSR when connected via Teinet.  dtr unasserted Does not assert DTR.	write	Stores the current configuration in permanent memory.
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 to match remote DSR when connected via Tainet.  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 commands  cirsorn Clears the screen.  default dtr Restores default DTR control, asserted while connected.  dtr continuously asserted  dtr continuously asserted  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted  Does not assert DTR.  exit Returns to the tunnel level.  Does not assert DTR to match remote DSR when connected via Telnet.  dtr unasserted Does not assert DTR.  exit Returns to the unnel level.  Displays the current configuration.  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  cirsorn Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Write Scores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  cirsorn Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Does not assert DTR.  Returns to the tunnel level.	serial (tunnel-serial:13) level commands	
dtr asserted while connected  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR regardless of any connections.  dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  show  Displays the current configuration.  Show history  Displays the last 20 commands entered during the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands  cirsom  Clears the screen.  default dtr  Restores default DTR control, asserted while connected dir unasserted while connected is active.  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Resturns to the tunnel level.  Displays the last 20 commands entered during the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands  cirsom  Clears the screen.  default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Returns to the tunnel level.  Show  Displays the last 20 commands entered during the current CLI session.  Serial (tunnel-serial:11) level commands  cirsom  Clears the screen.  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR regardless of any connections.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Clears the screen.  default dtr  Asserts DTR to match remote DSR when connected via Telnet.  Clears the screen.  default dtr  Asserts DTR to match remote DSR when connected via Telnet.  Does not assert DTR.  Returns to the tunnel level.	clrscrn	Clears the screen.
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 last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands cirscrn Clears the screen.  default dtr Restores default DTR control, asserted while connected.  dtr continuously asserted Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr unasserted Does not assert DTR. exit Returns to the tunnel level.  show Displays the last 20 commands entered during the current configuration in permanent memory.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted 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 last 20 commands entered during the current CLI session.  write Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  cirscrn Clears the screen.  default dtr Restores default DTR control, asserted while connected.  dtr asserted while connected Asserts DTR menever a connect or accept mode tunnel connection is active.  dtr continuously asserted Asserts DTR regardless of any connections.  dtr truport 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  Does not assert DTR.	default dtr	Restores default DTR control, asserted while connected.
dtr truport  Asserts DTR to match remote DSR when connected via Teinet.  dtr unasserted  Does not assert DTR.  exit  Returns to the tunnel level.  show  Displays the current configuration.  bisplays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Serial (tunnel-sorial:12) 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.  dtr truport  Asserts DTR to match remote DSR when connected via Teinet.  dtr unasserted  Does not assert DTR.  Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  clrscrn  Clears the screen.  Getauth DTR control, asserted while connected via Teinet.  Stores the current configuration.  Displays the last 20 commands entered during the current CLI session.  Write  Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  clrscrn  Clears the screen.  Clears the screen.  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 menever a connect or accept mode tunnel connection is active.  dtr continuously asserted  Asserts DTR regardless of any connections.  dtr truport  Asserts DTR regardless of any connections.  dtr unasserted  Does not assert DTR.  exit  Returns to the tunnel level.	dtr asserted while connected	
Telnet.  dtr unasserted Does not assert DTR.  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 commands  clirscrn 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 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 commands  clirscrn Clears the screen.  default dtr Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connected via Telnet.  Asserts DTR regardless of any connection in permanent memory.  Serial (tunnel-serial:11) level commands  clirscrn Clears the screen.  default dtr Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr asserted while connected Asserts DTR regardless of any connections.  dtr truport Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Resturns to the tunnel level.	dtr continuously asserted	Asserts DTR regardless of any connections.
exit Returns to the tunnel level.  show Displays the current configuration.  brown 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 commands  clirscrn 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 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.  Displays the last 20 commands entered during the current CLI session.  write Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) level commands  clirscrn 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 regardless of any connections.  dtr truport Clears the screen 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.	dtr truport	
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 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:11) 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 Clears the tunnel level.	dtr unasserted	Does not assert DTR.
show history  Displays the last 20 commands entered during the current CLI session.  Stores the current configuration in permanent memory.  Serial (tunnel-serial:12) level commands  Clears the screen.  default dtr  default dtr  Restores default DTR control, asserted while connected.  Asserts DTR whenever a connect or accept mode tunnel connection is active.  dtr continuously asserted  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Returns to the tunnel level.  show  Displays the last 20 commands entered during the current CLI session.  Write  Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) 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.  Asserts DTR regardless of any connections.  dtr continuously asserted  Asserts DTR regardless of any connections.  dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  Does not assert DTR to match remote DSR when connected via Telnet.  Does not assert DTR.  Returns to the tunnel level.	exit	Returns to the tunnel level.
write Stores the current configuration in permanent memory.  Serial (tunnel-serial:12) 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.  Returns to the tunnel level.  show Displays the current configuration.  bisplays the last 20 commands entered during the current CLI session.  write Stores the current configuration in permanent memory.  Serial (tunnel-serial:11) 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 regardless of any connections.  dtr truport Asserts DTR to match remote DSR when connected via Telnet.  Does not assert DTR.  Returns to the tunnel level.	show	Displays the current configuration.
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 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.  Returns to the tunnel level.	show history	
clrscrn  default dtr  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 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.	write	Stores the current configuration in permanent memory.
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 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.	serial (tunnel-serial:12) level commands	
dtr asserted while connected  Asserts DTR whenever a connect or accept mode tunnel connection is active.  Asserts DTR regardless of any connections.  Asserts DTR to match remote DSR when connected via Telnet.  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 commands  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.	clrscrn	Clears the screen.
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 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.	default dtr	Restores default DTR control, asserted while connected.
dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  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 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.  Returns to the tunnel level.	dtr asserted while connected	
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 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.	dtr continuously asserted	Asserts DTR regardless of any connections.
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 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.	dtr truport	
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 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.	dtr unasserted	Does not assert DTR.
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 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.  Returns to the tunnel level.	exit	Returns to the tunnel level.
CLI session.  write Stores the current configuration in permanent memory.  serial (tunnel-serial:11) 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.
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 history	
clrscrn  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.	write	Stores the current configuration in permanent memory.
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.	serial (tunnel-serial:11) level commands	
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.  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  Returns to the tunnel level.	clrscrn	Clears the screen.
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.	default dtr	Restores default DTR control, asserted while connected.
dtr truport  Asserts DTR to match remote DSR when connected via Telnet.  dtr unasserted  Does not assert DTR.  exit  Returns to the tunnel level.	dtr asserted while connected	
Telnet.  dtr unasserted Does not assert DTR.  exit Returns to the tunnel level.	dtr continuously asserted	Asserts DTR regardless of any connections.
exit Returns to the tunnel level.	dtr truport	
	dtr unasserted	Does not assert DTR.
show Displays the current configuration.	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 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:9) 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:8) 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: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	<u> </u>
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	The second secon
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	
clrscrn	Clears the screen.
default relay port	Restores the SMTP relay port to its default.
exit	Exits to the configuration level.
no relay address	Removes the SMTP relay address.
relay address <text></text>	Sets an SMTP relay address to direct all outbound email messages through a mail server.
relay port <number></number>	Sets the SMTP relay port.
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.
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.
show history	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	Restores the default maximum allowed concurrent incom-
	ing SSH sessions.
default port	Restores the default local port to the SSH server.
exit	Exits to the CLI level.
max sessions <number></number>	Sets the maximum allowed concurrent incoming SSH sessions.
	<number> = number of sessions.</number>
port <number></number>	Sets the local port that the SSH server uses. <number> = local port number.</number>
show	Displays the current configuration.
show history	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.
write	Stores the current configuration in permanent memory.
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.
write syslog (config-syslog) level commands	Stores the current configuration in permanent memory.
	Stores the current configuration in permanent memory.  Clears the screen.
syslog (config-syslog) level commands	
syslog (config-syslog) level commands clrscrn	Clears the screen.
syslog (config-syslog) level commands clrscrn default remote port	Clears the screen.  Restores the default syslog remote port.
syslog (config-syslog) level commands clrscrn default remote port default severity log level	Clears the screen.  Restores the default syslog remote port.  No logging.
syslog (config-syslog) level commands clrscrn default remote port default severity log level exit	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient.
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.</text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host</text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when mak-</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number></number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level critical</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert severity log level critical severity log level debug</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log all events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level critical  severity log level debug  severity log level emergency</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.  Log all events.  Log only Emergency events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level critical  severity log level debug  severity log level emergency  severity log level error</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.  Log only Emergency events.  Log only Emergency events.  Log only Error and more severe events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level critical  severity log level debug  severity log level emergency  severity log level error  severity log level information</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.  Log only Emergency events.  Log only Error and more severe events.  Log only Information and more severe events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level debug  severity log level debug  severity log level emergency  severity log level error  severity log level information  severity log level none</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port.  <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.  Log only Emergency events.  Log only Emergency events.  Log only Information and more severe events.  No logging.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level critical  severity log level debug  severity log level emergency  severity log level error  severity log level information  severity log level none  severity log level notice</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.  Log only Emergency events.  Log only Error and more severe events.  Log only Information and more severe events.  No logging.  Log only Notice and more severe events.</number></text>
syslog (config-syslog) level commands  clrscrn  default remote port  default severity log level  exit  host <text>  no host  remote port <number>  severity log level alert  severity log level critical  severity log level debug  severity log level emergency  severity log level error  severity log level information  severity log level none  severity log level notice  severity log level warning</number></text>	Clears the screen.  Restores the default syslog remote port.  No logging.  Returns to the config level.  Sets the address of the syslog recipient. <text> = IP address or name of the host.  Removes the address of the syslog recipient.  Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.  Log only Alert and more severe events.  Log only Critical and more severe events.  Log only Emergency events.  Log only Error and more severe events.  Log only Information and more severe events.  No logging.  Log only Warning and more severe events.</number></text>

	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	J
authentication disable	No password required for Telnet users.
authentication enable	Challenges the Telnet user with a password.
clrscrn	Clears the screen.
default max sessions	Restores the default maximum allowed concurrent incoming Telnet sessions.
default port	Restores the default local port to the Telnet server.
exit	Exits to the CLI level.
max sessions <number></number>	Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions.</number>
port <number></number>	Sets the local port that the Telnet server uses. <number> = local port number.</number>
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the Telnet statistics.
state disable	Disables the Telnet Server.
state enable	Enables the Telnet Server.
write	Stores the current configuration in permanent memory.
terminal 1 (config-terminal:1) 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".
default terminal type echo disable	
	Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back
echo disable	Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back
echo disable echo enable	Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.
echo disable echo enable exit	Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit
echo disable  echo enable  exit  exit connect menu disable	Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit to the CLI.  On the login connect menu, inserts the menu item allowing the user to exit
echo disable  echo enable  exit  exit connect menu disable  exit connect menu disable	Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit to the CLI.  On the login connect menu, inserts the menu item allowing the user to exit to the CLI.  Enters the line level.

	menu rather than the
no send break	CLI immediately after logging in.  Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current set-
preview connect menu	tings.
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. <li>line&gt; = number of the terminal line (serial port) to be configured.</li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
write	Stores the current configuration in permanent memory.
terminal 10 (config-terminal:10) level commands	
break duration <milliseconds></milliseconds>	Sets how long a break should last when it is being sent to the line.
	<pre><milliseconds> = number of milliseconds.</milliseconds></pre>
clrscrn	111111111111111111111111111111111111111
clrscrn default break duration	<milliseconds> = number of milliseconds.</milliseconds>
	<pre><milliseconds> = number of milliseconds.</milliseconds></pre> Clears the screen.
default break duration	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms).</milliseconds>
default break duration default terminal type	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back</milliseconds>
default break duration default terminal type echo disable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back</milliseconds>
default break duration default terminal type echo disable echo enable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line.</milliseconds>
default break duration default terminal type echo disable echo enable exit	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit</milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit</milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable exit connect menu disable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit to the CLI. Enters the line level.</milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable exit connect menu enable line	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit to the CLI. Enters the line level. <li><li><li><li><li><li><li><li><li><li< td=""></li<></li></li></li></li></li></li></li></li></li></milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable exit connect menu enable line <li>login connect menu disable</li>	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit to the CLI. Enters the line level. <li><li><li><li><li><li><li><li></li><!--</td--></li></li></li></li></li></li></li></milliseconds>

	tings.
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. <pre><li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li></pre>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
write	Stores the current configuration in permanent memory.
terminal 11 (config-terminal:11) 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	Enters the line level. <pre><li><li>&lt; = number of the line (serial port) to be configured.</li></li></pre>
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</text>

	hex. A control character has the form <control>C.</control>
	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.
terminal <line></line>	Enters the configure-terminal level. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
write	Stores the current configuration in permanent memory.
terminal 12 (config-terminal:12) 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	Enters the line level. <li><li><li><ne>= number of the line (serial port) to be configured.</ne></li></li></li>
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.</control></text>
	A decimal value character has the form \99. A hex value character has the form 0xFF.

show	Diaplaya the current configuration
	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. <pre><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></pre>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the line (serial port) to be configured.</li></li>
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.

<pre><li><li>= number of the terminal line (serial port) to be con- figured.</li></li></pre>
Enters the configure-terminal level for the network.
Sets the terminal type.
Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
Stores the current configuration in permanent memory.
Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
Clears the screen.
Restores the break duration to the default value (500 ms).
Sets the default terminal type, "UNKNOWN".
Disables echoing of characters received on the line back to the line.
Enables echoing of characters received on the line back to the line.
Exits to the configuration level.
On the login connect menu, removes the menu item allowing the user to exit to the CLI.
On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
Enters the line level. <li>  Ine&gt; = number of the line (serial port) to be configured.</li>
Disables the login connect menu, so a user will get the CLI immediately after logging in.
Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
Removes the configured send break character.
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, 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>
Displays the current configuration.
Displays the last 20 commands entered during the current CLI session.
021 000010111
Enters the configure-terminal level. <li>line&gt; = number of the terminal line (serial port) to be configured.</li>
Enters the configure-terminal level. <li><li><li>&lt; = number of the terminal line (serial port) to be con-</li></li></li>

tunnel <li>line&gt;</li>	Enters the tunnel level. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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	Enters the line level. <li><li><li>= number of the line (serial port) to be configured.</li></li></li>
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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
write	Stores the current configuration in permanent memory.

terminal 16 (config-terminal:16) 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	Enters the line level. <li><li><li>= number of the line (serial port) to be configured.</li></li></li>
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>	Enters the configure-terminal level. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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. <li><li><li>= number of the line (serial port) to be configured.</li></li></li>
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>	Enters the configure-terminal level. <li><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
write	Stores the current configuration in permanent memory.
terminal 3 (config-terminal:3) 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.  Exits to the configuration level.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit to the CLI.  On the login connect menu, inserts the menu item allowing the user to exit to the CLI.  Enters the line level.  Iline > Enters the line level.  Ilines = number of the line (serial port) to be configured.  Iogin connect menu disable  Disables the login connect menu, so a user will get the CLI immediately after logging in.  Iogin connect menu enable  Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.  In one send break  Removes the configured send break character.  Shows the layout of the connect menu with current settings.  Sets the optional send break character.  Sets the optional send break character.  It 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 OxFF.  Displays the current configuration.  Show bistory  Displays the last 20 commands entered during the currer CLI session.  Enters the configure-terminal level.  Iline> = number of the terminal line (serial port) to be configured.  Iterminal   Iterminal   Iters the configure-terminal level for the network.  Enters the tunnel level.  Inne> = number of the tunnel line (serial port) to be configured.  Write  Sotes the current configuration in permanent memory.  Enters the configuration in permanent memory.  Enters the current configuration in permanent memory.  Enters the current configuration in permanent memory.  Externinal 4 (config-terminal 4) level commands  break duration <miliseconds>  Sets how long a break should last when it is being sent to the line.</miliseconds>		to the line.
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.  Enters the line level.  Iline > Enters the line level.  Ilines = number of the line (serial port) to be configured.  Iogalia connect menu disable  Disables the login connect menu, so a user will get the CLI immediately after logging in.  Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.  Preview connect menu  Shows the layout of the connect menu with current settings.  Sets the optional send break character.  Sets the optional send break character.  Sets the character.  The character may be input as text, control, decimal, or hex.  A control character has the form very.  A control character has the form very.  A control character has the form very.  Show  Displays the current configuration.  Displays the last 20 commands entered during the current current configured.  Enters the configure-terminal level.  Inches = number of the terminal line (serial port) to be configured.  Enters the configure-terminal level for the network.  Sets the terminal type.  Enters the configure-terminal level for the network.  Sets the terminal type.  Enters the configure-terminal level for the network.  Sets the terminal type.  Enters the unnel level.  Inches = number of the tunnel line (serial port) to be configured.  Enters the configure-terminal level for the network.  Sets the unnel level.  Inches = number of the tunnel line (serial port) to be configured.  Enters the configuration in permanent memory.	echo enable	_
lowing the user to exit to the CLI.	exit	Exits to the configuration level.
ing the user to exit to the CLI.  line <li>line </li> <li>line = number of the line (serial port) to be configured.</li> <li>login connect menu disable</li> <li>Disables the login connect menu, so a user will get the CLI immediately after logging in.</li> <li>login connect menu enable</li> <li>Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.</li> <li>no send break</li> <li>Removes the configured send break character.</li> <li>Shows the layout of the connect menu with current settings.</li> <li>send break <control></control></li> <li>Sets the optional send break character.</li> <li>text&gt; = the character.</li> <li>text&gt; = the character.</li> <li>the character may be input as text, control, decimal, or hex.</li> <li>A control character has the form oxFF.</li> <li>show</li> <li>Displays the current configuration.</li> <li>show bitstory</li> <li>Displays the current configuration.</li> <li>show bitstory</li> <li>Displays the last 20 commands entered during the currer CLI session.</li> <li>terminal <iine></iine></li> <li>Enters the configure-terminal level.</li> <li>cline&gt; = number of the terminal line (serial port) to be configured.</li> <li>terminal type <text></text></li> <li>tenters the configure-terminal level for the network.</li> <li>terminal type.</li> <li>tenters the tunnel level.</li> <li>cline&gt; = number of the tunnel line (serial port) to be configured.</li> <li>write</li> <li>Stores the current configuration in permanent memory.</li> <li>torminal 4 (config-terminal-4) level commands</li>	exit connect menu disable	lowing the user to exit
cline> = 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>   Sets the optional send break character.     the character may be input as text, control, decimal, or hex.     A control character has the form \(\frac{1}{2}\)     A hex value character has the form \(\frac{1}{2}\)     A hex value character has the form \(\frac{1}{2}\)     Show   Displays the current configuration.     Show history   Displays the current configuration.     Displays the last 20 commands entered during the current configured.     Centers the configure-terminal level.     cline> = number of the terminal line (serial port) to be configured.     Sets the terminal type   Sets the terminal line (serial port) to be configured.     Sets the terminal type.   Sets the turnel line (serial port) to be configured.     Stores the current configuration in permanent memory.	exit connect menu enable	ing the user to exit
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.  Removes the configured send break character.  Shows the layout of the connect menu with current settings.  Sets the optional send break character.  Send break <control>  Sets the optional send break 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 OxFF.  Show  Displays the last 20 commands entered during the current cLI session.  Enters the configure-terminal level.  &lt; </control></control>	line <li>line&gt;</li>	
menu rather than the CLI immediately after logging in.  Removes the configured send break character.  Shows the layout of the connect menu with current settings.  Sets the optional send break character.  Sets 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 OxFF.  Show  Displays the current configuration.  Displays the last 20 commands entered during the current CLI session.  terminal <li>line&gt;  Enters the configure-terminal level.  <li>line&gt; = number of the terminal line (serial port) to be configured.  terminal type <text>  Sets the terminal type.  Enters the tunnel level.  <li>line&gt; = number of the tunnel line (serial port) to be configured.  Sets the tunnel level.  <li>line&gt; = number of the tunnel line (serial port) to be configured.  Sets the tunnel level.  <li>line&gt; = number of the tunnel line (serial port) to be configured.  Sets the tunnel level.  <li>line&gt; = number of the tunnel line (serial port) to be configured.  Sets the current configuration in permanent memory.  terminal 4 (config-terminal:4) level commands  break duration <milliseconds>  Sets how long a break should last when it is being sent to the line.</milliseconds></li></li></li></li></text></li></li></control>	login connect menu disable	CLI immediately
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, control, decimal, or hex. A control character has the form <pre></pre></text>	login connect menu enable	menu rather than the
tings.  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 0xFF.  Show  Displays the current configuration.  Displays the last 20 commands entered during the currer CLI session.  terminal <li>line&gt; Enters the configure-terminal level. <li>line&gt; = number of the terminal line (serial port) to be configured.  terminal type <text> Sets the terminal type.  Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.  Sets the terminal type.  Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.  Sets the tunnel level. <li>sets the current configuration in permanent memory.  **The character. The character. The character. The character. The character has the form vent vent vent vent vent vent vent vent</li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></text></li></li></control></text>	no send break	Removes the configured send break character.
	preview connect menu	
show history  Displays the last 20 commands entered during the currer CLI session.  Enters the configure-terminal level. <li><li><li><li><li><li><li><li><li><li></li></li></li></li></li></li></li></li></li></li>	send break <i><control></control></i>	<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.</control></text>
terminal      CLI session.       terminal      Enters the configure-terminal level. <li><li><li>line&gt; = number of the terminal line (serial port) to be configured.       terminal network     Enters the configure-terminal level for the network.       terminal type      Sets the terminal type.       tunnel      Enters the tunnel level.       <li><li><li><li><li><li>= number of the tunnel line (serial port) to be configured.       write     Stores the current configuration in permanent memory.       terminal 4 (config-terminal:4) level commands       break duration      Sets how long a break should last when it is being sent to the line.</li></li></li></li></li></li></li></li></li>	show	Displays the current configuration.
<pre>cline&gt; = number of the terminal line (serial port) to be configured.  terminal network  terminal type <text>  Sets the terminal type.  tunnel <li>line&gt; = number of the terminal level for the network.  Sets the terminal type.  Enters the tunnel level.</li></text></pre>	show history	Displays the last 20 commands entered during the current CLI session.
terminal type <text>  Sets the terminal type.  Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.  write  Stores the current configuration in permanent memory.  terminal 4 (config-terminal:4) level commands  break duration <milliseconds>  Sets how long a break should last when it is being sent to the line.</milliseconds></li></text>	terminal <line></line>	<li><li>&lt; = number of the terminal line (serial port) to be con-</li></li>
tunnel <li>tunnel <li>line&gt;  Enters the tunnel level.  <li>line&gt; = number of the tunnel line (serial port) to be configured.  Write  Stores the current configuration in permanent memory.  terminal 4 (config-terminal:4) level commands  break duration <milliseconds>  Sets how long a break should last when it is being sent to the line.</milliseconds></li></li></li>	terminal network	Enters the configure-terminal level for the network.
<pre></pre>	terminal type <text></text>	
terminal 4 (config-terminal:4) level commands break duration <milliseconds>  Sets how long a break should last when it is being sent to the line.</milliseconds>	tunnel <li>line&gt;</li>	<pre><li><li>= number of the tunnel line (serial port) to be con-</li></li></pre>
break duration <milliseconds>  Sets how long a break should last when it is being sent to the line.</milliseconds>	write	Stores the current configuration in permanent memory.
the line.	terminal 4 (config-terminal:4) level commands	
<pre> <milliseconds> = number of milliseconds.</milliseconds></pre>	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.	clrscrn	Clears the screen.
default break duration Restores the break duration to the default value (500 ms)	default break duration	Restores the break duration to the default value (500 ms).
default terminal type Sets the default terminal type, "UNKNOWN".	default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable  Disables echoing of characters received on the line back to the line.	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.	echo enable	=
exit Exits to the configuration level.	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. <pre><li><li>&lt;= number of the line (serial port) to be configured.</li></li></pre>
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. <li><li>&lt;= number of the terminal line (serial port) to be configured.</li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel	Enters the tunnel level. <pre><li><li>&lt; = number of the tunnel line (serial port) to be con-</li></li></pre>
	figured.
write	
terminal 5 (config-terminal:5) level commands	figured.  Stores the current configuration in permanent memory.
	figured.
terminal 5 (config-terminal:5) level commands	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line.
terminal 5 (config-terminal:5) level commands break duration < milliseconds>	figured.  Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
terminal 5 (config-terminal:5) level commands break duration <milliseconds>  clrscrn</milliseconds>	figured.  Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.</milliseconds>
terminal 5 (config-terminal:5) level commands break duration < milliseconds >  clrscrn default break duration	figured.  Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).</milliseconds>
terminal 5 (config-terminal:5) level commands break duration <milliseconds>  clrscrn default break duration default terminal type</milliseconds>	figured.  Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back</milliseconds>
terminal 5 (config-terminal:5) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable</milliseconds>	figured.  Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back</milliseconds>
terminal 5 (config-terminal:5) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable echo enable</milliseconds>	figured.  Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.</milliseconds>

	ing the user to exit to the CLI.
line	Enters the line level. <pre><li><li>&lt;= number of the line (serial port) to be configured.</li></li></pre>
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. <li>line&gt; = number of the terminal line (serial port) to be configured.</li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
write	Stores the current configuration in permanent memory.
terminal 6 (config-terminal:6) 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	Enters the line level. <li><li><li>&lt; = number of the line (serial port) to be configured.</li></li></li>

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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be con-</li>
	figured.
write	Stores the current configuration in permanent memory.
write terminal 7 (config-terminal:7) level commands	
- 12	
terminal 7 (config-terminal:7) level commands	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line.
terminal 7 (config-terminal:7) level commands break duration <milliseconds></milliseconds>	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn</milliseconds>	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration</milliseconds>	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type</milliseconds>	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable</milliseconds>	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable echo enable</milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable echo enable exit</milliseconds>	Stores the current configuration in permanent memory.  Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable echo enable exit exit connect menu disable</milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit to the CLI.  On the login connect menu, inserts the menu item allowing the user to exit</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable echo enable exit exit connect menu disable  exit connect menu enable</milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit to the CLI.  On the login connect menu, inserts the menu item allowing the user to exit to the CLI.  Enters the line level.</milliseconds>
terminal 7 (config-terminal:7) level commands break duration <milliseconds>  clrscrn default break duration default terminal type echo disable  echo enable  exit exit connect menu disable  exit connect menu enable  line <li>line <li>line&gt;</li></li></milliseconds>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).  Sets the default terminal type, "UNKNOWN".  Disables echoing of characters received on the line back to the line.  Enables echoing of characters received on the line back to the line.  Exits to the configuration level.  On the login connect menu, removes the menu item allowing the user to exit to the CLI.  On the login connect menu, inserts the menu item allowing the user to exit to the CLI.  Enters the line level.  <li><li><li><li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li>&lt;</li></li></li></li></li></milliseconds>

	menu rather than the
no cond brook	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. <li><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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.
	<pre><milliseconds> = number of milliseconds.</milliseconds></pre>
clrscrn	1
clrscrn default break duration	<milliseconds> = number of milliseconds.</milliseconds>
	<milliseconds> = number of milliseconds.  Clears the screen.</milliseconds>
default break duration	<milliseconds> = number of milliseconds.  Clears the screen.  Restores the break duration to the default value (500 ms).</milliseconds>
default break duration default terminal type	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back</milliseconds>
default break duration default terminal type echo disable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back</milliseconds>
default break duration default terminal type echo disable echo enable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line.</milliseconds>
default break duration default terminal type echo disable echo enable exit	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit</milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit</milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable exit connect menu disable	<milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit to the CLI. Enters the line level.</milliseconds>
default break duration default terminal type echo disable echo enable exit exit connect menu disable exit connect menu enable line	<pre><milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit to the CLI. Enters the line level. </milliseconds></pre> Cline> = number of the line (serial port) to be configured. Disables the login connect menu, so a user will get the CLI immediately
default break duration default terminal type echo disable echo enable exit exit connect menu disable exit connect menu enable line <li>login connect menu disable</li>	<pre><milliseconds> = number of milliseconds. Clears the screen. Restores the break duration to the default value (500 ms). Sets the default terminal type, "UNKNOWN". Disables echoing of characters received on the line back to the line. Enables echoing of characters received on the line back to the line. Exits to the configuration level. On the login connect menu, removes the menu item allowing the user to exit to the CLI. On the login connect menu, inserts the menu item allowing the user to exit to the CLI. Enters the line level. <li><li><li><li>line&gt; = number of the line (serial port) to be configured. Disables the login connect menu, so a user will get the CLI immediately after logging in. Enables the login connect menu, so a user will get the menu rather than the</li></li></li></li></milliseconds></pre>

	tings.
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>	Enters the configure-terminal level. <pre><li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li></pre>
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. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
write	Stores the current configuration in permanent memory.
terminal 9 (config-terminal:9) level comma	ands
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
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</text>

	T
	hex. A control character has the form <control>C. A decimal value character has the form \99.</control>
	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.
terminal <line></line>	Enters the configure-terminal level. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li><li><li>= number of the tunnel line (serial port) to be configured.</li></li></li>
write	Stores the current configuration in permanent memory.
terminal network (config-terminal:network) level comm	nands
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. <pre><li><li>&lt;= number of the line (serial port) to be configured.</li></li></pre>
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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
terminal type <text></text>	Sets the terminal type.
tunnel <li>line&gt;</li>	Enters the tunnel level. <pre><li><li>line&gt; = number of the tunnel line (serial port) to be configured.</li></li></pre>
write	Stores the current configuration in permanent memory.
trusted authorities (ssl-auth) level commands	
add	Adds an Authority Certificate.
clrscrn	Clears the screen.
exit	Exits to the ssl level.
no intermediate authority <cert></cert>	Removes an Intermediate Authority Certificate. <a cert="" href="https://www.ncerts.org/linearing-removes-at-10-12-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;no trusted authority &lt;cert&gt;&lt;/td&gt;&lt;td&gt;Removes a Trusted Authority Certificate. &lt;a href=" https:="">"&gt;</a> = index displayed by "show authority" command.
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></line>	Enters the line level. <pre><li><li>&lt;= number of the line (serial port) to be configured.</li></li></pre>
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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
	le , a , e , , , , , , , , , , , , , , ,
terminal network	Enters the configure-terminal level for the network.

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	Enters the line level. <pre></pre> <pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre></pre></pre>
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. <li>&lt;= number of the terminal line (serial port) to be configured.</li>
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
write	Stores the current configuration in permanent memory.
tunnel 11 (tunnel:11) 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. <pre><li></li></pre> <pre></pre> <pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre><pre></pre></pre>
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>	Enters the configure-terminal level. <pre><li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li></pre>
	Entere the configurate majoral level for the materials
terminal network	Enters the configure-terminal level for the network.

tunnel	Enters the tunnel level. <li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li>
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. <pre></pre>
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. <pre><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></pre>
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. <li><li><li>= number of the tunnel line (serial port) to be configured.</li></li></li>
write	Stores the current configuration in permanent memory.
tunnel 13 (tunnel:13) 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. <pre><li><li><li>= number of the line (serial port) to be configured.</li></li></li></pre>
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><li><li><li>= number of the terminal line (serial port) to be con-</li></li></li></pre>

	figured.
terminal network	Enters the configure-terminal level for the network.
tunnel	Enters the tunnel level. <iine> = number of the tunnel line (serial port) to be configured.</iine>
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. <pre><li><li><li>line&gt; = number of the line (serial port) to be configured.</li></li></li></pre>
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>	Enters the configure-terminal level. <li><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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	Enters the line level. <pre><li><li><li>line&gt; = number of the line (serial port) to be configured.</li></li></li></pre>
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.

terminal <li>Enters the configure-terminal level.</li>	show statistics	show connection statistics
cline> = number of the terminal line (serial port) to be configured.		
terminal network  tunnel <a href="https://dises-purple.com/figure-terminal level for the network.">https://dises-purple.com/figured.</a> Enters the tunnel level.    Aline> = 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 clear counters    Zeros all tunnel counters   Clears the screen.   Clears the screen.   Clears the disconnect level for this tunnel.   disconnect   Enters the disconnect level for this tunnel.   exit   Exits to the enable level.   Enters the line level.   exit   Exits to the enable level.   Enters the line level.		<pre><li><li>&lt; = number of the terminal line (serial port) to be con-</li></li></pre>
tunnel <in>tunnel <ine> Enters the tunnel level.  <inline> = 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   clorscrn Clears the screen.   connect Enters the disconnect level for this tunnel.   exit Exits to the enable level.   line <ime> = line  Enters the line level.   sine&gt; = number of the line (serial port) to be configured.   modern Enters the modern 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.   serial Enters the serial level for this tunnel.   show statistics show connection statistics   terminal <iine> Enters the configure-terminal level.   <ine> = number of the terminal line (serial port) to be configured.   terminal network Enters the configure-terminal level for the network.   tunnel <iiine> Enters the configure-terminal level for the network.   tunnel <iine> Enters the configure-terminal level for the network.   tunnel = number of the tunnel line (serial port) to be configured.   write Stores the current configuration in permanent memory.   tunnel = (lunnel:2) level commands   accept Enters the accept</iine></iiine></ine></iine></ime></inline></ine></in>	torminal natural	
cline> = number of the tunnel line (serial port) to be configured.   Stores the current configuration in permanent memory.		
ingured.  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  clear counters  clear counters  clear the screen.  connect Enters the disconnect level for this tunnel.  disconnect Enters the disconnect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the line level.  dine> Enters the modern level for this tunnel.  Enters the modern level for this tunnel.  Inner a number of the line (serial port) to be configured.  modern Enters the modern level for this tunnel.  Enters the packing level for this tunnel.  Enters the serial level for this tunnel.  Enters the configure-terminal level.  -{Inne> = number of the terminal line (serial port) to be configured.  Enters the configure-terminal level.  -{Inne> = number of the tunnel line (serial port) to be configured.  Enters the configure-terminal level for the network.  Enters the unnel level.  -{Inne> = number of the tunnel line (serial port) to be configured.  Enters the configure-terminal level for the network.  Enters the unnel level of the tunnel line (serial port) to be configured.  Enters the configure-terminal level for the network.  Enters the unnel level of the tunnel ine (serial port) to be configured.  Enters the unnel level of this tunnel.  Enters the unnel level of this tunnel.  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the line level.  -{Inne> = number of the line (serial port) to be configured.  Enters the disconnect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the disconnect level for this t	turiner	
tunnel 16 (tunnel:16) level commands accept		
auto show statistics show connection statistics clear counters clear counters Clears the screen.  connect Enters the connect level for this tunnel.  disconnect Enters the connect level for this tunnel.  disconnect Enters the disconnect level for this tunnel.  exit Exits to the enable level.  line <iniv> line &lt; line &gt; line (serial port) to be configured.  modem Enters the modem level for this tunnel.  con clear counters Unzeros all tunnel counters  packing Enters the packing level for this tunnel.  show history Displays the last 20 commands entered during the current CLI session.  show statistics show connection statistics terminal <iniv> line &gt; lenters the configure-terminal level.  <ini> lenters the configure-terminal level.  <ini> lenters the tunnel counters  Enters the configure-terminal level.  <ini> lenters the tunnel line (serial port) to be configured.  Enters the configure-terminal level for the network.  tunnel &lt; ini &gt; lenters the tunnel line (serial port) to be configured.  Enters the tunnel line (serial port) to be configured.  Enters the tunnel line (serial port) to be configured.  Enters the configuration in permanent memory.  tunnel 2 (tunnel-2) level commands  accept Enters the accept level for this tunnel.  disconnect Enters the screen.  connect Clears the screen.  connect Enters the screen.  connect Enters the connect level for this tunnel.  disconnect Enters the disconnect level for this tunnel.  exit Exits to the enable level.  <ini> lenters the line level.  <ini> lenters the l</ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></ini></iniv></iniv>	write	Stores the current configuration in permanent memory.
auto show statistics  clear counters  Clears the screen.  Enters the disconnect level for this tunnel.  disconnect  Exits to the enable level.  Exits to the enable level.  Exits to the enable level.  Enters the line level.	tunnel 16 (tunnel:16) level commands	
clear counters  clrscm  Clears the screen.  Clears the screen.  Clears the screen.  Clears the screen.  Connect  Enters the connect level for this tunnel.  disconnect  Exits to the enable level.  Exits to the enable level.  Exits to the enable level.  Exits the line level.  In exit   Exits the modern level for this tunnel.  In clear counters  Unzeros all tunnel counters  Exits the packing level for this tunnel.  Exits the packing level for this tunnel.  Exits 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.  In exit   Exits the configure-terminal level for the network.  Externinal exit   Exits the configure-terminal level for the network.  Externinal exit   Exits the tunnel level.  In exit   Exits the tunnel level.  In exit   Exits the tunnel level.  Exits the current configuration in permanent memory.  Externinal exit   Exits the accept level for this tunnel.  Externinal exit   Exits the screen.  Clears the screen.  Clears the screen.  Connect   Enters the screen.  Connect   Enters the disconnect level for this tunnel.  Exits to the enable level.  In exit   Exits to the enable level.  In exit   Exits to the enable level.  In exit   Exits the modern level for this tunnel.  Exits the modern level for this tunnel.  In exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.  Externing exit   Exits the modern level for this tunnel.	accept	Enters the accept level for this tunnel.
cirsorn  Clears the screen.  Cneed  Enters the connect level for this tunnel.  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Exits to the enable level.  Itine ≺line>  Enters the line level.  ⟨line> = number of the line (serial port) to be configured.  Modem  Enters the modem level for this tunnel.  Enters the modem level for this tunnel.  Unzeros all tunnel counters  packing  Enters the packing level for this tunnel.  Enters the packing level for this tunnel.  Show history  Displays the last 20 commands entered during the current CLI session.  Show statistics  show connection statistics  terminal <li>line&gt;  Enters the configure-terminal level.  ⟨line&gt; = number of the terminal line (serial port) to be configured.  Enters the configure-terminal level for the network.  Enters the tunnel level.  ⟨line&gt; = number of the tunnel line (serial port) to be configured.  Enters the tunnel level.  ⟨line&gt; = number of the tunnel line (serial port) to be configured.  Stores the current configuration in permanent memory.  ###################################</li>	auto show statistics	show connection statistics
connect Enters the connect level for this tunnel.  disconnect Enters the disconnect level for this tunnel.  Exits to the enable level.  Enters the line level.  Enters the line level.  Enters the line level.  Enters the line level.  Inne> = number of the line (serial port) to be configured.  Modem Enters the modem level for this tunnel.  No clear counters Unzeros all tunnel counters  Eaching Enters the packing level for this tunnel.  Enters the serial level for this tunnel.  Displays the last 20 commands entered during the current CLI session.  Show statistics Show connection statistics  Enters the configure-terminal level. <ine> = number of the terminal line (serial port) to be configured.  Enters the tunnel evel.  <ine> = number of the tunnel level for the network.  Enters the tunnel level.  <ine> = number of the tunnel line (serial port) to be configured.  Stores the current configuration in permanent memory.  **Tunnel 2 (tunnel-2) level commands**  accept Enters the accept level for this tunnel.  auto show statistics  clear counters  Zeros all tunnel counters  clears the connect level for this tunnel.  Enters the connect level for this tunnel.  Enters the connect level for this tunnel.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Enters the disconnect level for this tunnel.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Exits to the enable level.  <ine> = number of the line (serial port) to be configured.  Exits the modem level for this tunnel.  Exits the pack</ine></ine></ine></ine></ine></ine></ine></ine></ine></ine>	clear counters	Zeros all tunnel counters
disconnect Enters the disconnect level for this tunnel.  Exits to the enable level.  Enters the line level.  Enters the modern level for this tunnel.  no clear counters  Unzeros all tunnel counters  packing  Enters the serial 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. <in>enters the configure-terminal level.</in> <in>enters the configure-terminal level for the network.  Enters the configure-terminal level for the network.  Enters the tunnel level.  <ine> = number of the tunnel line (serial port) to be configured.  Enters the cunfigure-terminal level for the network.  Enters the cunfigure-terminal level for this tunnel.  Enters the cunfigure-terminal level for this tunnel.  Enters the configure-terminal level for this tunnel.  Enters the accept level for this tunnel.  Enters the connect level for this tunnel.  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the disconnect level for this tunnel.  Enters the line level.  «Inle» = number of the line (serial port) to be configured.  Enters the modern level for this tunnel.  Enters the modern level for this tunnel.</ine></in>	clrscrn	Clears the screen.
Exits to the enable level.    Ine    Enters the line level.	connect	Enters the connect level for this tunnel.
Enters the line level.    cline> = number of the line (serial port) to be configured.    modem	disconnect	Enters the disconnect level for this tunnel.
cline> = number of the line (serial port) to be configured.   modem	exit	Exits to the enable level.
Unzeros all tunnel counters  packing  Enters the packing level for this tunnel.  Enters the serial level for this tunnel.  Enters the serial level for this tunnel.  Displays the last 20 commands entered during the current CLI session.  Show statistics  show connection statistics  terminal <li>Enters the configure-terminal level. &lt;  line&gt; = number of the terminal line (serial port) to be configured.  Enters the configure-terminal level for the network.  tunnel <li>Enters the tunnel level. &lt;  line&gt; = number of the tunnel line (serial port) to be configured.  Enters the tunnel level for the network.  Enters the tunnel line (serial port) to be configured.  Stores the current configuration in permanent memory.  tunnel 2 (tunnel:2) level commands  accept  accept Enters the accept level for this tunnel.  auto show statistics  clear counters  Clear counters  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.  Einters the line level.  Einters the line level.  Einters the modem level for this tunnel.  Enters the modem level for this tunnel.</li></li>	line <li>line&gt;</li>	
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   sterminal  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> = 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   clrscm 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> = number of the line (serial port) to be configured.   modem Enters the modem level for this tunnel.   no clear counters Unzeros all tunnel counters   Enters the packing level for this tunnel.	modem	Enters the modem 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 <li>Enters the configure-terminal level. &lt;  line&gt; = number of the terminal line (serial port) to be configured.  terminal network Enters the configure-terminal level for the network.  tunnel </li> <li>### Enters the tunnel level. &lt;  line&gt; = number of the tunnel line (serial port) to be configured.  ### Stores the current configuration in permanent memory.  ### tunnel 2 (tunnel:2) level commands  ### accept</li>	no clear counters	Unzeros all tunnel counters
show history  Displays the last 20 commands entered during the current CLI session.  show statistics  show connection statistics  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.  Enters the configure-terminal level for the network.  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  clear counters  Clear counters  Clear ste screen.  Clears the screen.  connect  Enters the disconnect level for this tunnel.  disconnect  Enters the disconnect level for this tunnel.  Exits to the enable level.  <  line> = number of the line (serial port) to be configured.  The state of the line level.  <  line> = number of the line (serial port) to be configured.  **The state of the line level.  **Ine> = number of the line (serial port) to be configured.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for this tunnel.  **The state of the line level for thi	packing	Enters the packing level for this tunnel.
Show statistics  show connection statistics  terminal <li>Enters the configure-terminal level. <i line=""> = number of the terminal line (serial port) to be configured.</i></li> <li>terminal network</li> <li>Enters the configure-terminal level for the network.</li> <li>tunnel </li> <li>Enters the tunnel level. <i line=""> = number of the tunnel line (serial port) to be configured.</i></li> <li>write</li> <li>Stores the current configuration in permanent memory.</li> <li>tunnel 2 (tunnel:2) level commands</li> <li>accept</li> <li>Enters the accept level for this tunnel.</li> <li>auto show statistics</li> <li>show connection statistics</li> <li>clear counters</li> <li>Clears the screen.</li> <li>connect</li> <li>Enters the connect level for this tunnel.</li> <li>disconnect</li> <li>Enters the disconnect level for this tunnel.</li> <li>exit</li> <li>Exits to the enable level.</li> <li>line&gt; = number of the line (serial port) to be configured.</li> <li>modem</li> <li>Enters the modem level for this tunnel.</li> <li>Unzeros all tunnel counters</li> <li>Enters the packing level for this tunnel.</li>	serial	Enters the serial level for this tunnel.
terminal      Enters the configure-terminal level. <pre></pre>	show history	Displays the last 20 commands entered during the current CLI session.
cline> = number of the terminal line (serial port) to be configured.   terminal network	show statistics	show connection statistics
tunnel < line>  Enters the tunnel level.	terminal <line></line>	<pre><li><li>= number of the terminal line (serial port) to be con-</li></li></pre>
cline> = number of the tunnel line (serial port) to be configured.   write	terminal network	Enters the configure-terminal level for the network.
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 < line> Enters the line level.	tunnel <line></line>	<pre><li><li>= number of the tunnel line (serial port) to be con-</li></li></pre>
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> Enters the line level. < line> = number of the line (serial port) to be configured. modem Enters the modem level for this tunnel. Unzeros all tunnel counters packing Enters the packing level for this tunnel.	write	Stores the current configuration in permanent memory.
auto show statistics  clear counters  Clears the screen.  Connect  Connect  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Exit Exits to the enable level.  line   Enters the line level. <ine>line &lt; number of the line (serial port) to be configured.  Enters the modem level for this tunnel.  Unzeros all tunnel counters  Enters the packing level for this tunnel.</ine>	tunnel 2 (tunnel:2) level commands	
clear counters  clrscrn  Clears the screen.  Connect  disconnect  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Exit  Exits to the enable level.  line < line >  Enters the line level. < line> = number of the line (serial port) to be configured.  modem  Enters the modem level for this tunnel.  Unzeros all tunnel counters  packing  Enters the packing level for this tunnel.	accept	Enters the accept level for this tunnel.
connect  connect  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Exits to the enable level.  Enters the line level.  Enters the line level.  Iine < line> = number of the line (serial port) to be configured.  modem  Enters the modem level for this tunnel.  Unzeros all tunnel counters  packing  Enters the packing level for this tunnel.	auto show statistics	show connection statistics
connect  disconnect  Enters the connect level for this tunnel.  Enters the disconnect level for this tunnel.  Exits to the enable level.  line   Enters the line level.    Enters the line (serial port) to be configured.  modem  Enters the modem level for this tunnel.  Unzeros all tunnel counters  packing  Enters the packing level for this tunnel.	clear counters	Zeros all tunnel counters
disconnect  exit  Exits to the enable level.  line <li>line <li>exit  Enters the line level.  line &gt; = number of the line (serial port) to be configured.  modem  Enters the modem level for this tunnel.  Unzeros all tunnel counters  packing  Enters the packing level for this tunnel.</li></li>	clrscrn	Clears the screen.
exit Exits to the enable level.  line   Enters the line level. <ine> = 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.</ine>	connect	Enters the connect level for this tunnel.
line <li>line &gt; Enters the line level.</li> <li>line &gt; = number of the line (serial port) to be configured.</li> <li>modem</li> <li>Enters the modem level for this tunnel.</li> <li>Unzeros all tunnel counters</li> <li>packing</li> <li>Enters the packing level for this tunnel.</li>	disconnect	Enters the disconnect level for this tunnel.
<pre></pre>	exit	Exits to the enable level.
no clear counters  packing  Unzeros all tunnel counters  Enters the packing level for this tunnel.	line <li>line &gt;</li>	
packing Enters the packing level for this tunnel.	modem	Enters the modem level for this tunnel.
	no clear counters	Unzeros all tunnel counters
serial Enters the serial level for this tunnel.	packing	Enters the packing level for this tunnel.
	l	Fortune the constable colling this terms of

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal	Enters the configure-terminal level. <li><pre><li><pre></pre></li></pre><pre></pre><pre><pre>figured.</pre></pre></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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. <li><li>&lt;= number of the line (serial port) to be configured.</li></li>
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. <li><li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <li>line&gt;</li>	Enters the tunnel level. <pre><li><li>&lt;= number of the tunnel line (serial port) to be configured.</li></li></pre>
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
<u> </u>	

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. <li>line&gt; = number of the terminal line (serial port) to be configured.</li>
terminal network	Enters the configure-terminal level for the network.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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	Enters the line level. <li><li><li><li>= number of the line (serial port) to be configured.</li></li></li></li>
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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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. <li><li><li>= number of the line (serial port) to be configured.</li></li></li>

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. <li><li><li>= number of the terminal line (serial port) to be configured.</li></li></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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.
	<pre><li><li>= number of the line (serial port) to be configured.</li></li></pre>
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><li><li>line&gt; = number of the terminal line (serial port) to be configured.</li></li></pre>
terminal network	Enters the configure-terminal level for the network.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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. <li><li>&lt; = number of the line (serial port) to be configured.</li></li>
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. <li><li>&lt;= number of the terminal line (serial port) to be configured.</li></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <line></line>	Enters the tunnel level. <li>line&gt; = number of the tunnel line (serial port) to be configured.</li>
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	Enters the line level. <li>line&gt; = number of the line (serial port) to be configured.</li>
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. <li><li>&lt; = number of the terminal line (serial port) to be configured.</li></li>
terminal network	Enters the configure-terminal level for the network.
tunnel <li>line&gt;</li>	Enters the tunnel level. <li><li><li>= number of the tunnel line (serial port) to be configured.</li></li></li>
write	Stores the current configuration in permanent memory.
vip (config-vip) level commands	·
auto show counters	Displays VIP counters continuously.
auto show status	Displays VIP status continuously.
clear counters	Sets the VIP counters to zero.
clrscrn	Clears the screen.
exit	Exits to the configuration level.
	•

no clear counters	Restores the VIP counters to the aggregate values.
	55 5
show	Displays the current configuration.
show counters	Displays the VIP counters.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays the VIP status.
state disable	Disables use of Virtual IP (VIP) addresses.
state enable	Enables use of Virtual IP (VIP) addresses.
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 <group list=""></group>	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