LANTRONIX®

MatchPort® b/g Pro Embedded Device Server Command Reference

Part Number 900-534
Revision D May 2013

Copyright and Trademark

MatchPort® and Lantronix® are registered trademarks of Lantronix, Inc. in the United States and other countries. Evolution OS® is a registered trademark of Lantronix, Inc. in the United States. DeviceInstaller™ is a trademark of Lantronix, Inc.

Windows® and Internet Explorer® are registered trademark of Microsoft Corporation. Mozilla® and Firefox® are registered trademarks of the Mozilla Foundation. Chrome™ is a trademark of Google, Inc. 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: 949-450-7249

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

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide. For the latest revision of this product document, please check our online documentation at www.lantronix.com/support/documentation.

Revision History

Date	Rev.	Comments
April 2008	A	Initial Document
September 2008	B	Technical updates throughout, corresponding to firmware release 1.1.0.0.R6.
March 2009	C	Updated to firmware release 1.3.0.0R5, added bridging information.
May 2013	D	Updated to firmware release 5.2.0.3R2, adding wireless information.

Table of Contents

List of Figures

List of Tables

1: About This Guide

This guide describes how to configure the MatchPort® b/g Pro embedded 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 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

Chapter Summaries

This table lists and summarizes each chapter and appendix.

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 MatchPort b/g Pro.
Chapter 4: Configuration Using XML	Lists XCR groups and items and describes how to use XCRs to configure the MatchPort b/g Pro.
Chapter 5: Commands and Levels	Provides an index of the CLI Command Hierarchy with hyperlinks to the corresponding command details.

Conventions

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

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

Convention	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 web site at www.lantronix.com/support/documentation for the latest documentation and the following additional documentation.

Document	Description
MatchPort b/g Pro Embedded Device Server User Guide	Describes how to configure and use the MatchPort b/g Pro
MatchPort b/g Pro Embedded Device Server Integration Guide	Contains information about the MatchPort b/g Pro hardware, the MatchPort b/g Pro demonstration board, and integrating MatchPort into your product.
MatchPort b/g Pro Embedded Device Server Getting Started Guide	Describes how to get the MatchPort b/g Pro demonstration board up and running.
DeviceInstaller Online Help	Instructions for using the Lantronix Windows-based utility to locate the MatchPort b/g Pro and to view its current settings.
Secure Com Port Redirector User Guide	Instructions for using the Lantronix Windows-based utility to create secure virtual com ports.
Com Port Redirector Quick Start and Online Help	Instructions for using the Lantronix Windows-based utility to create virtual com ports.

2: Overview

Evolution OS® software is the Lantronix® cutting-edge operating system that supports three convenient configuration methods: Web Manager, Command Line Interface (CLI), and Extensible Markup Language (XML). For more information about the Web Manager, see the *MatchPort b/g Pro User Guide* at the Lantronix website.

XML Architecture and Device Control

XML is a fundamental building block for the future growth of Machine-to-Machine (M2M) networks. Evolution 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, Evolution OS uses industry-standard tools for configuration, communication, and control. For example, the Evolution OS 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 device server.

3: Command Line Interface

This chapter describes accessing the MatchPort® b/g Pro embedded device server by using Telnet, SSH, or serial ports to configure the MatchPort, 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 Ports*
- *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 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 DeviceInstaller. See the DeviceInstaller Online Help for more information, available on our website www.lantronix.com/support/downloads.

To access the MatchPort b/g Pro by using Telnet, perform the following steps.

1. Click **Start > Run**. The **Run** dialog box displays.
2. Type `cmd` in the dialog box and press **OK**.
3. Type `telnet x.x.x.x` (x.x.x.x is the IP address). The MatchPort b/g Pro 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 Ports

Serial Command 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.

Serial Recovery

In this mode, the normal boot process is interrupted, allowing recovery from unknown or incorrect configuration settings. While the back door is active, the CLI prompt is changed to “>>” (instead of “>”) and the Web Manager is inaccessible. These serve as an important indication that the device boot processes has been temporarily halted. To complete the boot process, terminate the serial CLI session (with the exit command).

To configure the Lantronix device server locally using a serial port, connect a terminal or a PC running a terminal emulation program to one of the device server's serial ports. Configure the terminal for 9600 baud, 8-bit, no parity, 1 stop bit, and no flow control.

1. Power off the device.
2. Press and hold down the exclamation point (!) key.
3. Power on the device. After about ten seconds, the exclamation point will display on the terminal or PC screen.
4. 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>#echo?` displays a list of all echo 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>#echo*` displays a list of all echo 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 Evolution OS operating system 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. 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:

- **Ctrl + a**: place cursor at the beginning of a line
- **Ctrl + b**: backspace one character
- **Ctrl + d**: delete one character
- **Ctrl + e**: place cursor at the end of the line
- **Ctrl + f**: move cursor forward one character
- **Ctrl + k**: delete from the current position to the end of the line
- **Ctrl + l**: redraw the command line
- **Ctrl + n**: display the next line in the history
- **Ctrl + p**: display the previous line in the history
- **Ctrl + u**: delete entire line and place cursor at start of prompt
- **Ctrl + w**: delete one word back
- **Ctrl + z**: a shortcut for the exit command
- **Esc + b**: move cursor back one word
- **Esc + f**: move cursor forward one word

Understanding the CLI Level Hierarchy

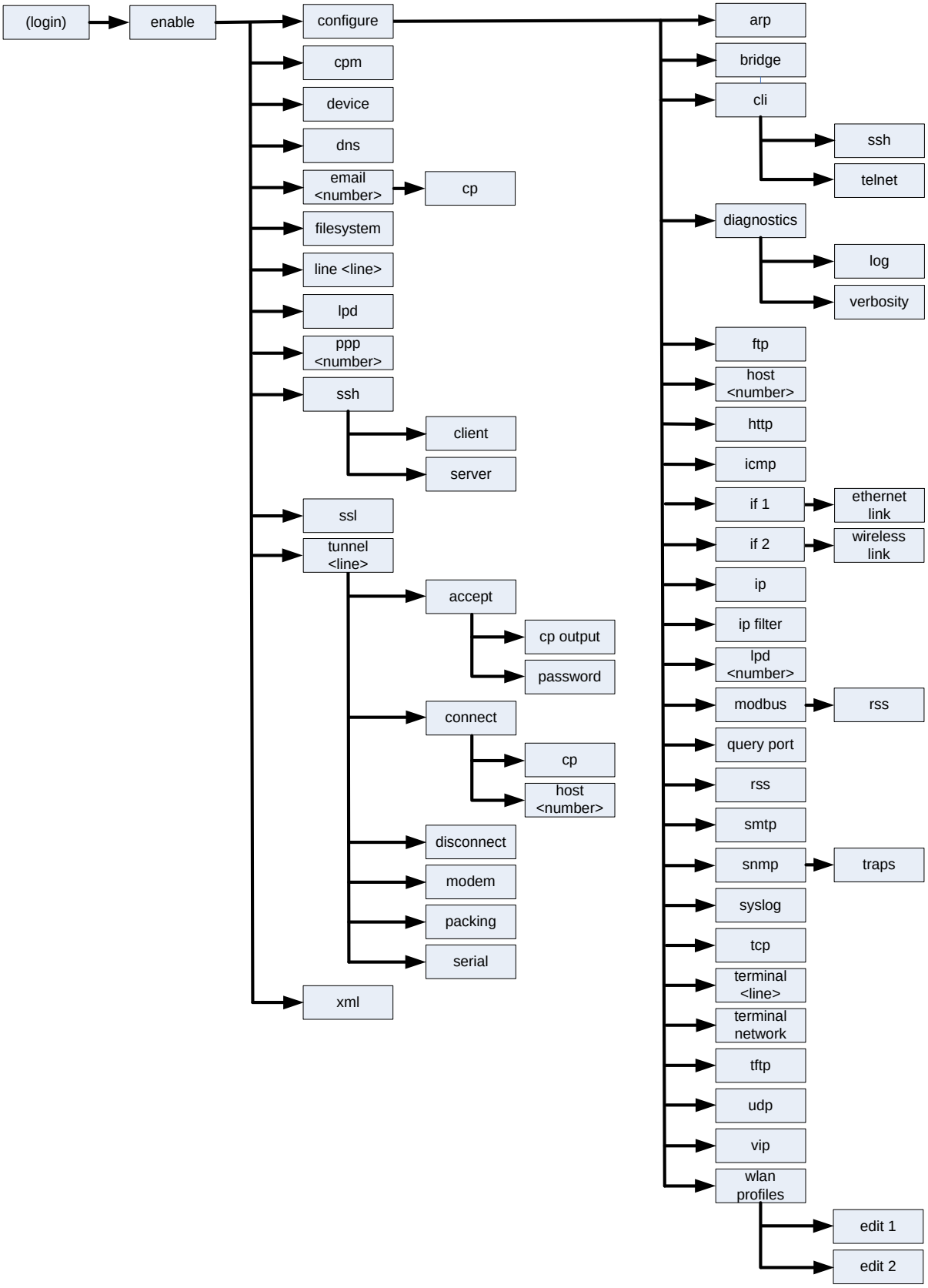
The CLI hierarchy is a series of levels. Arranging commands in a hierarchy of levels provides a way to organize and group similar commands, provide different levels of security, and reduce the complexity and number commands and options presented to a user at one time.

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 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 MatchPort b/g Pro is presented in *Figure 3-1*.

Figure 3-1 CLI Level Hierarchy



Commands at the login level, shown in *Figure 3-2*, do not affect current configuration settings and are not displayed initially. If you type <**?**>, you will see the login sub-commands. These commands provide diagnostic and status information only.

Figure 3-2 Login Level Commands

```
>?
clrscrn                                 enable
exit                                    ping <host>
ping <host> <count>                     ping <host> <count> <timeout>
show                                    show history
show matchport_bg_pro                   trace route <host>

>
```

To configure the MatchPort b/g Pro, you must be in the enable level and any of its sub-levels. *Figure 3-3* shows the enable level commands.

Figure 3-3 Enable Level Commands

```
>enable
(enable)#?
auto show interfaces                    auto show processes
clear interfaces counters               clrscrn
configure                               connect
connect line <line>                     cpm
device                                  disable
dns                                     email <number>
exit                                    filesystem
kill ssh <session>                      kill telnet <session>
line <line>                             lpd
no clear interfaces counters            ping <host>
ping <host> <count>                     ping <host> <count> <timeout>
ppp <line>                              reload
reload factory defaults                 show
show history                            show interfaces
show ip sockets                         show matchport_bg_pro
show processes                          show sessions
ssh                                     ssh <optClientUsername> <host>
ssh <optClientUsername> <host> <port>   ssl
telnet <host>                           telnet <host> <port>
trace route <host>                      tunnel <line>
write                                   xml

(enable)#
```

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

4: Configuration Using XML

The MatchPort® b/g Pro embedded 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 device server filesystem. 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 device server devices.

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 shown in *Figure 4-1*.

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>
]>
```

The 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.

Notes:

- *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 MatchPort b/g Pro User Guide for more information about the Web Manager 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

```
<?xml version="1.0" standalone="yes"?>
<configrecord>
 <configgroup name = "serial command mode" instance = "1">
      <configitem name = "mode">
             <value>disable</value>
      </configitem>
 </configgroup>
</configrecord>
```

The Evolution OS™ operating system 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>, <configgroup>, <configitem>, and <value> XML elements.

Figure 4-3 XML Group Example

```
<?xml version=”1.0” standalone=”yes”?>
<configrecord>
 <configgroup name = “serial command mode” instance = “1”>
      <configitem name = “mode”>
             <value>disable</value>
      </configitem>
 </configgroup>
</configrecord>
```

Figure 4-4 XML Example of Multiple Named Values

```
<?xml version=”1.0” standalone=”yes”?>
<configrecord>
 <configgroup name = “ssh server”
      <configitem name = “host rsa keys”>
          <value name = “public key”></value>
          <value name = “private key”></value>
      </configitem>
 </configgroup>
</configrecord>
```

Figure 4-5 XML Example of Multiple Items

```
<?xml version=”1.0” standalone=”yes”?>
<configrecord>
  <configgroup name = “email” instance = “1”>
      <configitem name = “to”>
            <value>john.doe@somewhere.com></value>
      </configitem>
      <configitem name = “from”>
            <value>evolution@matchportbg pro.com></value>
      </configitem>
 </configgroup>
</configrecord>
```

Figure 4-6 XML Example with Multiple Groups

```
<?xml version=”1.0” standalone=”yes”?>
<configrecord>
  <configgroup name = "ftp server">
       <configitem name = "state">
            <value>enable</value>
       </configitem>
       <configitem name = "admin username">
            <value>admin</value>
       </configitem>
       <configitem name = "admin password">
            <value><!-- configured and ignored --></value>
       </configitem>
  </configgroup>
  <configgroup name = "tftp server">
       <configitem name = "state">
            <value>enable</value>
       </configitem>
       <configitem name = "allow file creation">
            <value>disable</value>
       </configitem>
  </configgroup>
</configrecord>
```

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 *Best Practices* or the Filesystem Browser section in the *MatchPort b/g Pro User Guide*.
- CLI—XCRs can be imported (captured) or exported (dumped) directly to a Telnet, SSH, or serial line CLI session. Capturing an XCR can be started by pasting a valid XCR directly into the CLI prompt. Evolution OS 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 matchport_bg_pro.xcr is requested. On export (FTP get of matchport_bg_pro.xcr), the FTP server obtains the current XCR from Evolution OS and sends it as a file. On import (FTP put of matchport_bg_pro.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 file matchport_bg_pro.xcr is not read from or written to the file system. See FTP in the *MatchPort® b/g Pro Embedded 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 Evolution OS. 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.

Caution: ***The filename matchport_bg_pro.xsr.xcr is not acceptable, because performing a FTP get on that name produces the current configuration and does not perform an FTP from the filesystem. Also, the filename matchport_bg_pro.xsr.xsr is not acceptable, because performing an FTP get on that name produces the current status and does not get anything from the filesystem.***

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's 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 a 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 tunneling settings for port 1 and serial line 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, line:2"
```

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

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

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

```
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"
```

Passwords in the XML File

If you log in to a device server to which you will be pasting an XCR, you do not need to include passwords in the file, because you are already logged into the device. However, if you send an XCR to one or more devices that are password protected, you can include the appropriate passwords in the XCR and skip the login steps.

The “xml paste passwords” `<configgroup>` name is used with the “passwords” `<configitem>` name and “cli login” and “cli enable level” values to specify the passwords to use when the device has been configured with password protection. The password value is clear text. To protect the password, establish an SSH connection to the device server. *Figure 4-7* shows an example.

Figure 4-7 XML Example of Supplying Passwords

```
<!—To supply passwords when importing via cli capture -->
<configgroup name = "xml paste passwords">
        <configitem name = "passwords">
            <value name = "cli login"></value>
            <value name = "cli enable level"></value>
        </configitem>
</configgroup>
```

XML Configuration Groups

Table 4-8 lists the MatchPort b/g Pro XCR groups in alphabetical order. This table indicates the various group items, as well as some possible value names and options.

Note: *Any instance of **<** in the table may be read as **<** (the html encoded form for less than) and any instance of **>** may be read as **>** (the html encoded form for greater than).*

***Table 4-8* XCR Groups**

Group Name	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		
	timeout			Default: 60 seconds
bridge	state		enable, disable	
	bridging mac address			
cli	login password			Value is SECRET, hidden from user view.
	enable level password			Value is SECRET, hidden from user view.

Group Name	Group Item	Value Name	Value Options	Additional Information
cli (continued)	quit connect line			Accepts text containing control characters, for example, <control> A represents control-A Default: <control>L
	inactivity timeout		<None>, ...	Default: 15 minutes
cp group (Attribute of “instance” is required for the group name.)	state		enable	Changes state of the CP group.
			disable	
	cp (Attribute of “instance is a number.)	bit		Bit number
		type	input	
			output	
		assert low	enable	
			disable	
device	short name			
	long name			
	serial number			
	firmware version			Read only.
diagnostics	log	output	disable, filesystem, line <number>	Default: disable
		max length		Default: 50 Kbytes
		severity level	debug, information, notice, warning, error	Default: debug
	verbosity	wlan topic		
		wlan detail		
email (Attribute of “instance” is a number.)	to			Multiple addresses may be separated with semicolons.
	cc			Multiple addresses may be separated with semicolons.
	from			
	reply to			
	subject			
	message file			
	overriding domain			
	server port			Default: 25
	local port		<Random>, ...	Default: <Random>

Group Name	Group Item	Value Name	Value Options	Additional Information
email (Attribute of “instance” is a number.) (continued)	priority		urgent, high, normal, low, very low	Default: normal
	cp	group		
		trigger value		
ethernet (Attribute of “instance” is “eth0”.)	speed		auto, 10, 100	Default: auto
	duplex		auto, half, full	Default: auto
ftp server	state		enable, disable	Default: enable
	admin username			Default: admin
	admin password			Value is SECRET, hidden from user view.
host (Attribute of “instance” is a number.)	name			
	protocol		telnet, ssh	Default: telnet
	ssh username			
	remote address			
	remote port			Default: 0
http authentication uri (Attribute of “instance” is the URI.)	user delete	name		Deletes an HTTP Authentication URI user. The value element is used to specify the user for deletion.
	realm			
	type			
	user (Attribute of “instance” is the user name.)	password		
http server	state		enable, disable	Default: enable
	port		<None>, ...	Default: 80
	secure port		<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
	max timeout			Default: 10 seconds
	max bytes			Default: 40960
	logging state		enable, disable	Default: enable
	max log entries			Default: 50

Group Name	Group Item	Value Name	Value Options	Additional Information
http server (continued)	log format			Default: %h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"
	authentication timeout			Default: 30 minutes
icmp	state		enable, disable	Default: enable
interface (Attribute of “instance” is “eth0” or “wlan0”)	bootp		enable, disable	Default: disable
	dhcp		enable, disable	Default: enable
	ip address		<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>, ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	hostname			
	domain			
	dhcp client id			Set the identity of the client device.
	primary dns		<None>, ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	secondary dns		<None>, ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	state		enable, disable	
ip	multicast time to live			Default: 1 hops
	ip time to live			

Group Name	Group Item	Value Name	Value Options	Additional Information
ip filter	delete entries		enable, disable	If enabled, deletes any existing entries before adding “filter entry”.
	filter delete	ip address		Deletes a specific IP filter entry.
		net mask		Deletes a specific IP filter entry.
	filter entry	ip address		If configured, is a specific IP address.
		net mask		If configured, is a specific net mask.
line (Attribute of “instance” is a number.)	name			
	interface		rs232, rs485 half-duplex, rs485 full-duplex	Default:
	state		enable, disable	Default: depends on instance
	protocol		none, tunnel, ppp, lpd	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
	xoff char			Accepts a control character, for example, <control> A represents control-A Default: <control>S
	gap timer		<None>, ...	Default: none
	threshold			Default: 56 bytes

Group Name	Group Item	Value Name	Value Options	Additional Information
modbus	tcp server state		enable, disable	Default: disable
	additional port		<None>, ...	Default: <None>
	response timeout			Default: 3000 milliseconds
	rss	trace input	enable, disable	Default: disable
power management	state		enable, disable	
ppp (Attribute of “instance” is a number.)	local ip		<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).
	peer ip		<None>), ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	authentication mode		none, pap, chap, ms-chap, ms-chapv2	Default: none
	username			
	password			Value is SECRET, hidden from user view.
query port	state		enable, disable	
rss	feed		enable, disable	Default: disable
	persist		enable, disable	Default: disable
	max entries			Default: 100
serial command mode (Attribute of “instance” is a number.)	mode			
	echo serial string			
	serial string			
	signon message			
	wait time			
	cp	group		
		trigger value		

Group Name	Group Item	Value Name	Value Options	Additional Information
snmp	state		enable, disable	Default: enable
	read community			Value is SECRET, hidden from user view. Default: public
	write community			Value is SECRET, hidden from user view. Default: private
	system contact			
	system name			Default: <Default>
	system description			Default: <Default>
	system location			
	traps	state	enable, disable	Default: enable
		primary destination		
		secondary destination		
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 (Attribute of “instance” is required for the known host name)	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		
	client user (Attribute of “instance” is required for the user name)	password		
		remote command		
		public rsa key		
		private rsa key		
		public dsa key		
		private dsa key		

Group Name	Group Item	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			
	authorized user delete	name		
	authorized user (Attribute of “instance” is required for the authorized user name)	password		
		public rsa key		
		public dsa key		
ssl	RSA certificate	certificate		Enter the text of the certificate.
		private key		Enter the text of the private key. If configured and not exporting secrets, exports only a placeholder.
	DSA certificate	certificate		Enter the text of the certificate.
		private key		Enter the text of the private key. If configured and not exporting secrets, exports only a placeholder.
	trusted ca		enable, disable	
	delete all cas		enable, disable	If enabled, deletes any existing trusted cas before adding “trusted ca”.
syslog	state		enable, disable	Default: disable
	host			
	local port			Default: 514
	remote port			Default: 514
	severity log level		none, emergency, alert, critical, error, warning, notice, information, debug	Default: none
tcp	resets		enable, disable	Default: enable
	ack limit			Number of packets received before an ACK is forced. Default: 3 packets
	send data		standard, expedited	Default: standard

Group Name	Group Item	Value Name	Value Options	Additional Information
tcp (continued)	max retrans			
	max retrans syn ack			
	send data			
telnet	state		enable, disable	Default: enable
	port			Default: 23
	max sessions			Default: 3
terminal (Attribute of “instance” is either “network” or a number.)	terminal type			Default: UNKNOWN
	login connect menu		enable, disable	Default: disable
	exit connect menu		enable, disable	Default: disable
	send break			Accepts a control character, for example, <control> A represents control-A
	break duration			Default: 500 milliseconds
	echo		enable, disable	Default: enable
tftp server	state		enable, disable	Default: enable
	allow file creation		enable, disable	Default: disable
	allow firmware update		enable, disable	Default: disable
	allow xcr import		enable, disable	Default: disable
tunnel accept (Attribute of “instance” is a number.)	accept mode		disable, always, any character, start character, modem control asserted, modem emulation	Default: always
	local port		<None>, ...	Default: <None>
	protocol		tcp, ssh, telnet, tcp aes, ssl	Default: tcp
	tcp keep alive		<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

Group Name	Group Item	Value Name	Value Options	Additional Information
tunnel accept (Attribute of “instance” is a number.) (continued)	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>, ...	Default: <None>
	email disconnect		<None>, ...	Default: <None>
	cp output	group		
		connection value		
		disconnection value		
tunnel connect (Attribute of “instance” 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
	flush start character		enable, disable	Default: enable
	local port		<Random>, ...	Default: <Random>
	host (Attribute of “instance” is a number.)	vip	enable, disable	Default: disable
		vip name		
		address		
		port		
		protocol		
		ssh username		
		validate certificate		
		tcp keep alive	<Random>, ...	
		aes encrypt key		
		aes decrypt key		
	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

Group Name	Group Item	Value Name	Value Options	Additional Information
tunnel connect (Attribute of “instance” is a number.) (continued)	email connect		<None>, ...	Default: <None>
	email disconnect		<None>, ...	Default: <None>
	cp output	goup	connection value, disconnection value	
tunnel disconnect (Attribute of “instance” is a number.)	stop character			Accepts a control character, for example, <control> A represents control-A
	flush step character		enable, disable	Default: disable
	modem control		enable, disable	Default: disable
	timeout			Default: 0 milliseconds
	flush serial		enable, disable	Default: disable
tunnel modem (Attribute of “instance” is a number.)	echo pluses		enable, disable	Default: disable
	echo commands		enable, disable	Default: enable
	verbose response		enable, disable	Default: enable
	response type		text, numeric	Default: text
	error unknown commands		enable, disable	Default: disable
	incoming connection		disabled, automatic, manual	Default: disabled
	connect string			
	display remote ip		enable, disable	Default: disable
tunnel packing (Attribute of “instance” is a number.)	packing mode		disable, timeout, send character	Default: disable
	timeout			Default: 1000 milliseconds
	threshold			Default: 512 bytes
	send character			Accepts a control character, for example, <control> A represents control-A Default: <control>M
	trailing character			Accepts a control character, for example, <control> A represents control-A

Group Name	Group Item	Value Name	Value Options	Additional Information
tunnel serial (Attribute of “instance” is a number.)	dtr		asserted while connected, continuously asserted, unasserted, truport	Default: asserted while connected
vip	state		enable, disable	default: disable
wlan	choice (Attribute of an “instance” is a number)	default_infrastructure_profile		
		default_adhoc_profile		
		profile		
	out of range scan interval			
	roaming		enable, disable	
wlan profile(Attribute of an “instance” is “default_ adhoc_profile” or “default_infrastructure_profile”)	basic	network name		
		topology		
		channel		
	advanced	adhoc merging	enable, disable	
		tx data rate maximum		
		tx data rate		
		tx power maximum		
		tx power		
		tx retries		
		power management	enable, disable	
		power management interval		

Group Name	Group Item	Value Name	Value Options	Additional Information
wlan profile(Attribute of an “instance” is “default_ adhoc_profile” or “default_infrastructure_profile”) (continued)	security	suite		
		key type		
		passphrase		
		wep authentication		
		wep key size		
		wep tx key index		
		wep key 1		
		wep key 2		
		wep key 3		
		wep key 4		
		wpax authentication		
		wpax key		
		wpax ieee 802.1x		
		wpax eap-ttls option		
		wpax peap option		
		wpax username		
		wpax password		
		wpax encryption		
		wpax validate certificate	enable, disable	
xml import control	restore factory configuration			
	delete cpm groups		enable, disable	
	cpm group delete	name		
	delete wlan profiles		enable, disable	
	wlan profile delete			
	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 4-9 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.

Currently, the only XSR groups that contain any sub groups are buffer pools and tunnel. The buffer pools group has the following sub groups:

- Protocol stack
- Ethernet driver
- Line

The tunnel group has the following sub groups:

- Tunnel Modem

Table 4-9 **XSR Groups and Items**

Group Name	Item Name	Value Name	Valid Values
arp (Attribute of “instance” is “eth0”.)	arp entry	ip address	
		mac address	
		age	
		type	dynamic
			static
bridge	enable state		
	active state		
buffer pool	this group contains other groups: ethernet driver, protocol stack		
device	product info	product type	
		serial number	
		firmware version	
		uptime	
		permanent config	saved
			unsaved
	region		
email (Attribute of “instance” is a number.)	success	sent	
		sent with retries	
	failed		
	queued		
email log (Attribute of “instance” is a number.)	entry	time	
		log	

Group Name	Item Name	Value Name	Valid Values
ethernet driver (Within group “buffer pool”.)	buffer headers	total	
		free	
		used	
		max used	
	cluster pool	cluster size	
		total	
		free	
		used	
		max used	
filesystem	filesystem size		
	available space		
	clean space		
	dirty space		
	file and dir space used		
	data space used		
	number of files		
	number of directories		
	number of system files		
	opened files		
	locked files		
	opened for sharing		
	banks	current	A
			B
		firmware begin	
		firmware end	
		firmware erase cycles	
		bank a begin	
		bank a end	
		bank a erase cycles	
		bank b begin	
		bank b end	
		bank b erase cycles	
	busy		yes
			no

Group Name	Item Name	Value Name	Valid Values
ftp	status		running
			inactive
	connections	rejected	
		accepted	
	last client	ip address	
		port	
hardware	cpu	type	
		speed	
	memory	flash size	
		ram size	
http	state		enabled
			disabled
	logging	entries	
		bytes	
http log	entry (Attribute of “instance” is a number.)		
	totals	entries	
		bytes	

Group Name	Item Name	Value Name	Valid Values
icmp	in	messages	
		messages discarded	
		errors	
		destination unreachable	
		time exceeded messages	
		parameter problems	
		source quench requests	
		redirects	
		ping requests	
		ping replies	
		timestamp requests	
		timestamp replies	
		address mask requests	
		address mask replies	
	out	messages	
		messages discarded	
		errors	
		destination unreachables	
		time exceeded messages	
		parameter problems	
		source quench requests	
		redirects	
		ping requests	
		ping replies	
		timestamp requests	
		timestamp replies	
		address mask requests	
		address mask replies	

Group Name	Item Name	Value Name	Valid Values
interface (Attribute of “instance” is “eth0”.)	generic	status	no link
			link up
			disabled
			unknown
		errors	(error text)
			none
	ethernet (Present only for eth0.)	speed	10
			100
		duplex	full
			half
	arp	encapsulation	ARPA
		type	ARPA
		timeout	
	default gateway		
	network mask		
	domain		
	mac address		
	hostname		
	ip address		
	last change		
	mtu		
	primary dns		
	secondary dns		

Group Name	Item Name	Value Name	Valid Values
interface (Attribute of “instance” is “eth0”.) (Continued.)	transmit	octets	
		unicast	
		non unicast	
		discards	
		errors	
		broadcast packets	
		multicast packets	
		filtered packets	
		deferred	
		multiple retries	
		one retry	
		underflows	
		late collisions	
		retry errors	
		carrier lost errors	
	receive	octets	
		unicast	
		non unicast	
		discards	
		errors	
		broadcast packets	
		multicast packets	
		filtered packets	
		unknown protocol	
		framing errors	
		overflows	
		crc errors	
		missed frame errors	
interface (Attribute of an “instance” is “wlan0”)	generic	status	
		errors	
ip	state		enabled
			disabled
	default ttl		
	forwarded		
	route discards		

Group Name	Item Name	Value Name	Valid Values
interface (Attribute of an “instance” is “wlan0”) (continued)	in	receives	
		header errors	
		address errors	
		unknown protocols	
		discarded	
		delivered	
	out	requests	
		discards	
		discards no route	
	reassembly	timeout	
		needed	
		success	
		failures	
ip sockets	ip socket	protocol	UDP
			TCP
		rx queue	
		tx queue	
		local address	
		local port	
		remote address	
		remote port	
		state	

Group Name	Item Name	Value Name	Valid Values
line (Attribute of “instance” is a number.)	receiver	bytes	
		breaks	
		parity errors	
		framing errors	
		overrun errors	
		no receive buffer errors	
		queued bytes	
		flow control	n/a
			stop
			go
	transmitter	bytes	
		breaks	
		queued bytes	
		flow control	n/a
			stop
			go
	line levels	cts	asserted
			not asserted
		rts	asserted
			not asserted
		dsr	asserted
			not asserted
		dtr	asserted
			not asserted
line (With no instance.) (Within group “line” with instance.)	state		enable
			disable
	protocol		tunnel
			none
			ppp
	baud rate		Any value from 300 to 230400.
	parity		even
			none
			odd
	data bits		7
			8
	stop bits		1
			2

Group Name	Item Name	Value Name	Valid Values
line (With no instance.) (Within group “line” with instance.) (continued)	flow control		hardware
			none
			software
	xon char		
	xoff char		
memory	main heap	condition	clean
			corrupt
		total memory	
		available memory	
		fragments	
		allocated blocks	
processes	process (Attribute of “instance” is a number.)	cpu %	
		stack used	
		stack size	
		thread name	
protocol stack (within group “buffer pool”)	buffer headers	total	
		free	
		used	
		max used	
	cluster pool	cluster size	
		total	
		free	
		used	
		max used	
query port	status		enabled
			disabled
	last connection	ip address	
		port	
	in	discoveries	
		unknown queries	
		erroneous packets	
	out	discovery replies	
		errors	
rss	url		
	data	entries	
		bytes	
sessions	fragments	needed	
		failures	
		success	

Group Name	Item Name	Value Name	Valid Values
ssh	state		active
			waiting
			disabled
	totals	uptime	
		bytes in	
		bytes out	
tcp	retransmission	algorithm	vanj
		timeout minimum	
		timeout maximum	
	connections	maximum	
		open active	
		open passive	
		failed	
		resets	
		established	
	errors in		
	resets	in	
		out	
	segments	in	
		out	
		retransmitted	
telnet	state		active
			waiting
			disabled
	totals	uptime	
		bytes in	
		bytes out	
	last connection	local ip address	
		local port	
		remote ip address	
		remote port	
tftp	downloaded		
	uploaded		
	not found		
	errors	read	
		write	
		unknown	
	last client	ip address	
		port	

Group Name	Item Name	Value Name	Valid Values
tunnel (Attribute of “instance” is a number.)	aggregate	completed connects	
		completed accepts	
		disconnects	
		dropped connects	
		dropped accepts	
		octets from serial	
		octets from network	
		connect connection time	
		accept connection time	
		connect dns address changes	
		connect dns address invalids	
tunnel modem (within group “tunnel”)	echo commands		enable
			disable
	verbose response		enable
			disable
	response type		text
			numeric
	error unknown commands		disable
			enable
	incoming connection		disabled
			automatic
			manual
udp	in unknown ports		
	in datagrams		
	in errors		
	out datagrams		
xsr	out	bytes	
		lines	
		elements	
	errors		

5: Commands and Levels

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

- snmp (config-snmp)
  - traps (config-snmp-traps)
- syslog (config-syslog)
- tcp (config-tcp)
- terminal 1 (config-terminal:1)
- terminal 2 (config-terminal:2)
- terminal network (config-terminal:network)
- tftp (config-tftp)
- udp (config-udp)
- vip (config-vip)
- wlan profiles (config-profiles)
  - edit 1 (config-profile-basic:default_adhoc_profile)
    - advanced (config-profile-advanced:default_adhoc_profile)
      - security (config-profile-security:default_infrastructure_profile)
        - advanced (config-profile-advanced:default_infrastructure_profile)
        - wep (config-profile-security-wep:default_infrastructure_profile)
          - key 1 (config-profile-security-wep-key:default_infrastructure_profile:1)
          - key 2 (config-profile-security-wep-key:default_infrastructure_profile:2)
          - key 3 (config-profile-security-wep-key:default_infrastructure_profile:3)
          - key 4 (config-profile-security-wep-key:default_infrastructure_profile:4)
        - wpax (config-profile-security-wpax:default_infrastructure_profile)
      - security (config-profile-security:default_adhoc_profile)
        - wep (config-profile-security-wep:default_adhoc_profile)
          - key 1 (config-profile-security-wep-key:default_adhoc_profile:1)
          - key 2 (config-profile-security-wep-key:default_adhoc_profile:2)
          - key 3 (config-profile-security-wep-key:default_adhoc_profile:3)
          - key 4 (config-profile-security-wep-key:default_adhoc_profile:4)
        - wpax (config-profile-security-wpax:default_adhoc_profile)
    - edit 2 (config-profile-basic:default_infrastructure_profile)
- cpm (cpm)
- device (device)

Table 5-1 Commands and Levels

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 <*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*>	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.
cp output	Enters the next lower level.
default accept mode	Restores the default accept mode as "always".
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.
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.
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*>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
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 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.
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*>	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.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in 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*>	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*>	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.
cp output	Enters the next lower level.
default accept mode	Restores the default accept mode as "always".
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.
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.
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*>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
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 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.
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*>	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.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
write	Stores the current configuration in permanent memory.
advanced (config-profile-advanced:default_infrastructure_profile) level commands	
adhoc merging disable	Disables ad hoc merging.
adhoc merging enable	Enables ad hoc merging.
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
basic	Switch to basic level
clrscrn	Clears the screen.
default power management interval	Restores the power management interval to the default value (1 beacon).
default tx data rate	Restores the TX data rate to the default value (auto-reduction).
default tx data rate maximum	Restores the maximum TX data rate to the default value (54 Mbps).
default tx power	Restores TX power to the default value (Fixed).
default tx power maximum	Restores the maximum TX power to the default value (14 dBm).
default tx retries	Restores TX retries to the default value (7).
exit	Exit to the profiles level
power management disable	Disables power management.
power management enable	Enables power management.
power management interval <*beacons (100 ms each)*>	Sets the power management time interval in beacons. (A

	beacon is 100 msec.)
security	Switch to security level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
tx data rate auto-reduction	Enables TX data rate auto-reduction.
tx data rate fixed	Enables a fixed data rate.
tx data rate maximum 1 mbps	Sets the data rate maximum to 1 Mbps.
tx data rate maximum 11 mbps	Sets the data rate maximum to 11 Mbps.
tx data rate maximum 12 mbps	Sets the data rate maximum to 12 Mbps.
tx data rate maximum 18 mbps	Sets the data rate maximum to 18 Mbps.
tx data rate maximum 2 mbps	Sets the data rate maximum to 2 Mbps.
tx data rate maximum 24 mbps	Sets the data rate maximum to 24 Mbps.
tx data rate maximum 36 mbps	Sets the data rate maximum to 36 Mbps.
tx data rate maximum 48 mbps	Sets the data rate maximum to 48 Mbps.
tx data rate maximum 5.5 mbps	Sets the data rate maximum to 5.5 Mbps.
tx data rate maximum 54 mbps	Sets the data rate maximum to 54 Mbps.
tx data rate maximum 6 mbps	Sets the data rate maximum to 6 Mbps.
tx data rate maximum 9 mbps	Sets the data rate maximum to 9 Mbps.
tx power adaptation	Enables power adaptation.
tx power fixed	Enables fixed power.
tx power maximum <*dBm*>	Sets the TX power maximum in dBm. <dBm> = measure of power in decibels with respect to one milliwatt.
tx retries <*number*>	Sets the number of retries.
write	Stores the current configuration in permanent memory.
advanced (config-profile-advanced:default_adhoc_profile) level commands	
adhoc merging disable	Disables ad hoc merging.
adhoc merging enable	Enables ad hoc merging.
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
basic	Switch to basic level
clrscrn	Clears the screen.
default power management interval	Restores the power management interval to the default value (1 beacon).
default tx data rate	Restores the TX data rate to the default value (auto-reduction).
default tx data rate maximum	Restores the maximum TX data rate to the default value (54 Mbps).
default tx power	Restores TX power to the default value (Fixed).
default tx power maximum	Restores the maximum TX power to the default value (14 dBm).
default tx retries	Restores TX retries to the default value (7).
exit	Exit to the profiles level
power management disable	Disables power management.
power management enable	Enables power management.
power management interval <*beacons (100 ms each)*>	Sets the power management time interval in beacons. (A beacon is 100 msec.)
security	Switch to security level

show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
tx data rate auto-reduction	Enables TX data rate auto-reduction.
tx data rate fixed	Enables a fixed data rate.
tx data rate maximum 1 mbps	Sets the data rate maximum to 1 Mbps.
tx data rate maximum 11 mbps	Sets the data rate maximum to 11 Mbps.
tx data rate maximum 12 mbps	Sets the data rate maximum to 12 Mbps.
tx data rate maximum 18 mbps	Sets the data rate maximum to 18 Mbps.
tx data rate maximum 2 mbps	Sets the data rate maximum to 2 Mbps.
tx data rate maximum 24 mbps	Sets the data rate maximum to 24 Mbps.
tx data rate maximum 36 mbps	Sets the data rate maximum to 36 Mbps.
tx data rate maximum 48 mbps	Sets the data rate maximum to 48 Mbps.
tx data rate maximum 5.5 mbps	Sets the data rate maximum to 5.5 Mbps.
tx data rate maximum 54 mbps	Sets the data rate maximum to 54 Mbps.
tx data rate maximum 6 mbps	Sets the data rate maximum to 6 Mbps.
tx data rate maximum 9 mbps	Sets the data rate maximum to 9 Mbps.
tx power adaptation	Enables power adaptation.
tx power fixed	Enables fixed power.
tx power maximum <*dBm*>	Sets the TX power maximum in dBm. <dBm> = measure of power in decibels with respect to one milliwatt.
tx retries <*number*>	Sets the number of retries.
write	Stores the current configuration in permanent memory.
arp (config-arp) level commands	
add <*ip address*> <*MAC address*>	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.
clrscrn	Clears the screen.
default timeout	Restores the default ARP cache timeout.
exit	Exits to the configuration level.
remove all	Removes all entries from the ARP cache.
remove ip <*ip address*>	Removes an entry from the ARP cache. <ip address> = address of the entry being removed.
show	Displays the current configuration.
show cache	Displays the ARP cache table.
show history	Displays the last 20 commands entered during the current CLI session.
timeout <*seconds*>	Sets the ARP cache timeout. <seconds> = ARP cache timeout in seconds.
write	Stores the current configuration in permanent memory.
bridge 1 (config-bridge:bridge0) level commands	
bridging mac address <*hexadecimal*>	Sets the Bridging MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
clrscrn	Clears the screen.

exit	Exits to the config level.
no bridging mac address	Removes the Bridging MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Show bridge statistics
show status	Show bridge status
state disable	Disables bridging.
state enable	Enables bridging.
write	Stores the current configuration in permanent memory.
choice 1 (config-wlan-choice:wlan0:1) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile *<text>*	Selects a profile. <text> = name of the profile.
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.
choice 2 (config-wlan-choice:wlan0:2) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile *<text>*	Selects a profile. <text> = name of the profile.
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.
choice 3 (config-wlan-choice:wlan0:3) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile *<text>*	Selects a profile. <text> = name of the profile.
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.
choice 4 (config-wlan-choice:wlan0:4) level commands	
apply wlan	Try out WLAN settings without saving them to Flash.

	If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile *<text>*	Selects a profile. <text> = name of the profile.
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.
cli (config-cli) level commands	
clrscrn	Clears the screen.
default inactivity timeout	The default inactivity timeout will apply to CLI sessions.
default quit connect line	Restores the default string used to quit the "connect line <line>" command.
enable level password *<text>*	Sets the enable-level password.
exit	Exits to the configuration level.
inactivity timeout *<minutes>*	Sets the inactivity timeout for all CLI sessions.
login password *<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.
no login password	Removes the CLI login password.
quit connect line *<control>*	Sets the string used to quit the "connect line <line>" command. The characters may be input as text or control. A control character has the form <control>C.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh	Change to menu level for SSH configuration and status.
telnet	Change to menu level for Telnet configuration and status.
write	Stores the current configuration in permanent memory.
client (ssh-client) level commands	
clrscrn	Clears the screen.
default user *<username>* command	Restore the user command to the default login shell
delete all known hosts	Remove all hnown hosts
delete all users	Remove all users
delete known host *<server>*	Remove known host
delete user *<username>*	Delete the named user
exit	Exits to the ssh level.
known host *<server>*	Set known host RSA or DSA key
no known host *<server>* dsa	Remove known host DSA key
no known host *<server>* rsa	Remove known host RSA key
no user *<username>* dsa	Remove user DSA key
no user *<username>* rsa	Remove user RSA key
show	Show SSH Client settings
show history	Displays the last 20 commands entered during the current CLI session.
show known host *<server>*	Show known host RSA and DSA keys

show user <*username*>	Show information for a user
user <*username*>	Set username and RSA or DSA keys
user <*username*> command <*command*>	Customizes the user command
user <*username*> generate dsa 1024	Generate DSA public and private keys
user <*username*> generate dsa 512	Generate DSA public and private keys
user <*username*> generate dsa 768	Generate DSA public and private keys
user <*username*> generate rsa 1024	Generate RSA public and private keys
user <*username*> generate rsa 512	Generate RSA public and private keys
user <*username*> generate rsa 768	Generate RSA public and private keys
user <*username*> password <*password*>	Set username with password and optional RSA or DSA keys
write	Stores the current configuration in permanent memory.
configure (config) level commands	
arp	Changes to the command level for ARP configuration and status.
bridge <*bridge*>	Changes to the bridge configuration level.
cli	Change to menu level for CLI configuration and status
clrscrn	Clears the screen.
diagnostics	Enters the diagnostics level.
exit	Exits to the enable level.
ftp	Enters the ftp level.
host <*number*>	Change to config host level
http	Enters the http level.
icmp	Changes to the command level for ICMP configuration and status.
if <*instance*>	Changes to the interface configuration level.
ip	Changes to the command level for IP configuration and status.
ip filter	Enters the config-filter level.
kill ssh <*session*>	Kills SSH session with index from "show sessions"
kill telnet <*session*>	Kills Telnet session with index from "show sessions"
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
modbus	Changes to the modbus configuration level.
power management state disable	Disables CPU Power Management.
power management state enable	Enables CPU Power Management.
query port	Enters the query port level.
rss	Change to menu level for RSS configuration and status
show	Displays system information.
show history	Displays the last 20 commands entered during the current CLI session.
show power management	Displays the current configuration.
smtp	Changes to the command level for SMTP configuration and status.
snmp	Enters the snmp level.
syslog	Enters the syslog level.
tcp	Changes to the command level for TCP configuration and status.
terminal <*line*>	Enters the configure-terminal level.

	<line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tftp	Enters the tftp level.
udp	Changes to the command level for UDP configuration and status.
vip	Change to menu level for VIP configuration and status
wlan profiles	Enters the WLAN profiles configuration level.
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.
cp output	Enters the next lower level.
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.
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.
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*>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <*number*>	Sets a specific port for use as the local port. <number> = the number of the port to use.
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <*number*>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <*milliseconds*>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in 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.
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.
cp output	Enters the next lower level.
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.
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.
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*>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <*number*>	Sets a specific port for use as the local port. <number> = the number of the port to use.
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.

no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <*number*>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <*milliseconds*>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in 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.
write	Stores the current configuration in permanent memory.
cp (email-cp:4) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
group <*text*>	Specify a CP group that shall trigger an email. <text> = configurable pin group.
no group	Disables the trigger to send an email.
no trigger value	Clears the value that shall trigger an email.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
trigger value <*number*>	Specify a value of the CP group that shall trigger an email. <number> = numeric value to watch for from the CP group. Can be specified as hex if prepended with “0x”.
write	Stores the current configuration in permanent memory.
cp (email-cp:3) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
group <*text*>	Specify a CP group that shall trigger an email. <text> = configurable pin group.
no group	Disables the trigger to send an email.
no trigger value	Clears the value that shall trigger an email.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
trigger value <*number*>	Specify a value of the CP group that shall trigger an email. <number> = numeric value to watch for from the CP group. Can be specified as hex if prepended with “0x”.
write	Stores the current configuration in permanent memory.
cp (email-cp:2) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.

group <*text*>	Specify a CP group that shall trigger an email. <text> = configurable pin group.
no group	Disables the trigger to send an email.
no trigger value	Clears the value that shall trigger an email.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
trigger value <*number*>	Specify a value of the CP group that shall trigger an email. <number> = numeric value to watch for from the CP group. Can be specified as hex if prepended with “0x”.
write	Stores the current configuration in permanent memory.
cp (email-cp:1) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
group <*text*>	Specify a CP group that shall trigger an email. <text> = configurable pin group.
no group	Disables the trigger to send an email.
no trigger value	Clears the value that shall trigger an email.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
trigger value <*number*>	Specify a value of the CP group that shall trigger an email. <number> = numeric value to watch for from the CP group. Can be specified as hex if prepended with “0x”.
write	Stores the current configuration in permanent memory.
cp output (tunnel-connect-cp_output:2) level commands	
clrscrn	Clears the screen.
connection value <*number*>	Sets the value to output to the CP Group upon connect mode connection. <number> = binary to output (typically 1 or 0).
default connection value	Restores the default value for connect mode connection.
default disconnection value	Restores the default value for connect mode disconnec-tion.
disconnection value <*number*>	Sets the value to output to the CP Group upon connect mode disconnection. <number> = binary to output (typically 1 or 0).
exit	Exits to the next higher level.
group <*text*>	Configures the CP Group to set upon making or breaking a connect mode connection. <text> = CP Group.
no group	Removes the CP Set Group for connect mode.
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.
cp output (tunnel-accept-cp_output:2) level commands	
clrscrn	Clears the screen.
connection value <*number*>	Sets the value to output to the CP Group upon accept mode connection.

	<number> = binary to output (typically 1 or 0).
default connection value	Restores the default value for accept mode connection.
default disconnection value	Restores the default value for accept mode disconnection.
disconnection value <*number*>	Sets the value to output to the CP Group upon accept mode disconnection. <number> = binary to output (typically 1 or 0).
exit	Exits to the next higher level.
group <*text*>	Configures the CP Group to set upon making or breaking an accept mode connection. <text> = CP Group.
no group	Removes the CP Set Group for accept mode.
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.
cp output (tunnel-connect-cp_output:1) level commands	
clrscrn	Clears the screen.
connection value <*number*>	Sets the value to output to the CP Group upon connect mode connection. <number> = binary to output (typically 1 or 0).
default connection value	Restores the default value for connect mode connection.
default disconnection value	Restores the default value for connect mode disconnec-tion.
disconnection value <*number*>	Sets the value to output to the CP Group upon connect mode disconnection. <number> = binary to output (typically 1 or 0).
exit	Exits to the next higher level.
group <*text*>	Configures the CP Group to set upon making or breaking a connect mode connection. <text> = CP Group.
no group	Removes the CP Set Group for connect mode.
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.
cp output (tunnel-accept-cp_output:1) level commands	
clrscrn	Clears the screen.
connection value <*number*>	Sets the value to output to the CP Group upon accept mode connection. <number> = binary to output (typically 1 or 0).
default connection value	Restores the default value for accept mode connection.
default disconnection value	Restores the default value for accept mode disconnection.
disconnection value <*number*>	Sets the value to output to the CP Group upon accept mode disconnection. <number> = binary to output (typically 1 or 0).
exit	Exits to the next higher level.
group <*text*>	Configures the CP Group to set upon making or breaking an accept mode connection. <text> = CP Group.
no group	Removes the CP Set Group for accept mode.

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.
cpm (cpm) level commands	
add <*cp*> to <*group*>	Adds the specified CP to the specified group. <cp> = configurable pin. <group> = the name of the group to which you want to add the CP.
add <*cp*> to <*group*> <*bit*>	Adds a specified CP to a specified group at a specified bit position. <cp> = configurable pin. <group> = the name of the group to which you want to add the CP. <bit> = bit position.
clrscrn	Clears the screen.
create <*group*>	Creates a configurable pin (CP) group. <group> = the name for the new group.
delete <*cp*> from <*group*>	Removes a CP from a specified group and sets the CP to its default configuration of input. <cp> = configurable pin. <group> = the name of the group.
delete <*group*>	Removes a group and resets all CPs in that group to the default configuration of input. <group> = the name of the group.
disable <*group*>	Disables the specified group. <group> = the name of the group.
enable <*group*>	Enables a disabled group. <group> = the name of the group.
exit	Exits to the enable level.
get <*group*>	Displays the value of the specified group. <group> = the name of the group.
set <*cp*> as input	Configures a CP as an asserted high input. <cp> = configurable pin.
set <*cp*> as input assert low	Configures a CP as an asserted low input. <cp> = configurable pin.
set <*cp*> as output	Configures a CP as an asserted high output. <cp> = configurable pin.
set <*cp*> as output assert low	Configures a CP as an asserted low output. <cp> = configurable pin.
set <*group*> <*value*>	Assigns a value to the specified group. <group> = the name of the group. <value> = numeric value to assign to the CP group. Can be specified as hex if prepended with “0x”.
show <*group*>	Displays group information for specified group. <group> = the name of the group.
show cp	Displays configuration and group information for all CPs.
show groups	Displays all groups defined and their state.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
device (device) level commands	

auto show tlog	Continuously displays the internal trouble log.
auto show upload	Continuously displays the status of firmware upload.
clrscrn	Clears the screen.
default long name	Restores the default product long name.
default short name	Restores the default product short name.
dhrystone	Runs the Dhrystone benchmark program.
exit	Exit to the enable level.
long name <*name*>	Sets the product long name, displayed in command mode and the Web interface.
short name <*name*>	Sets the product short name, displayed in command mode and the Web interface. <name> = maximum of eight characters.
show	Show system information
show buffer pool	Displays information about the various buffer pools.
show codefile memory	Displays memory utilization by code files.
show delta memory	Displays differences in memory utilization by code files or line reference.
show hardware information	Displays information about the hardware.
show history	Displays the last 20 commands entered during the current CLI session.
show linereference memory <*code filename*>	Displays memory utilization by line reference for one code file.
show matchport_bg_pro	Show system information
show memory	Displays current memory usage information.
show task memory	Displays task memory utilization.
show task state	Displays current task states.
show tlog	Displays the internal trouble log.
show upload	Displays the status of firmware upload.
write	Stores the current configuration in permanent memory.
diagnostics (config-diagnostics) level commands	
clrscrn	Clears the screen.
exit	Returns to the config level.
log	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
verbosity	Enters the next lower level.
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*>	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.
timeout <*milliseconds*>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in 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*>	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.
timeout <*milliseconds*>	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in 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*>	Return a lookup on the DNS name or IP address.
remove all	Removes all entries from the DNS Cache.

remove host <*host*>	Removes an entry from the DNS Cache.
show	Show DNS status and cache entries.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
edit 1 (config-profile-basic:default_adhoc_profile) level commands	
advanced	Switch to advanced level
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
channel <*number*>	Sets the radio channel for AdHoc. <number> = number of the radio channel.
clrscrn	Clears the screen.
default channel	Restores the default value to the radio channel.
default topology	Restores the default topology, which is Infrastructure.
exit	Exit to the profiles level
network name <*text*>	Sets the network name.
no network name	Clears the network name.
security	Switch to security level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
topology adhoc	Sets topology to Adhoc.
topology infrastructure	Sets topology to Infrastructure.
write	Stores the current configuration in permanent memory.
edit 2 (config-profile-basic:default_infrastructure_profile) level commands	
advanced	Switch to advanced level
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
channel <*number*>	Sets the radio channel for AdHoc. <number> = number of the radio channel.
clrscrn	Clears the screen.
default channel	Restores the default value to the radio channel.
default topology	Restores the default topology, which is Infrastructure.
exit	Exit to the profiles level
network name <*text*>	Sets the network name.
no network name	Clears the network name.
security	Switch to security level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
topology adhoc	Sets topology to Adhoc.
topology infrastructure	Sets topology to Infrastructure.
write	Stores the current configuration in permanent memory.
email 1 (email:1) level commands	
auto show statistics	Continuously displays email statistics.
cc <*text*>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.

clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
cp	Enters the next lower level.
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*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*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.
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*>	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.
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*>	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.
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*>	Sets the Subject for email alerts. <text> = text to placed as the subject.

to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 2 (email:2) level commands	
auto show statistics	Continuously displays email statistics.
cc <*text*>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
cp	Enters the next lower level.
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*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*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.
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*>	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.
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*>	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.
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*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 3 (email:3) level commands	
auto show statistics	Continuously displays email statistics.
cc <*text*>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
cp	Enters the next lower level.
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*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*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.
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*>	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.

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>*	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.
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>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 4 (email:4) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
cp	Enters the next lower level.
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>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<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.
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*>	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.
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*>	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.
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*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
enable (enable) level commands	
auto show interfaces	Show interface statistics
auto show processes	Continuously show thread runtime information
clear interfaces counters	Zeros interface session counters
clrscrn	Clears the screen.
configure	Enters the configuration level.
connect	Show name and number for lines.
connect line <*line*>	Begin session on serial port.
cpm	Enters the CP Manager level.
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"
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
lpd	Enters the lpd level.

no clear interfaces counters	Unzeros interface session counters
ping <*host*>	Ping destination continuously with 5 second timeout
ping <*host*> <*count*>	Ping destination n times with 5 second timeout
ping <*host*> <*count*> <*timeout*>	Ping destination n times with x timeout (in seconds)
ppp <*line*>	Enters the serial line PPP level.
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 matchport_bg_pro	Show system information
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>. 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.
ssl	Enters the SSL configuration level.
telnet <*host*>	Begin telnet session on network <host>.
telnet <*host*> <*port*>	Begin telnet session on network <host>:<port>.
trace route <*host*>	Trace route to destination
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xml	Enters the XML level.
filesystem (filesystem) level commands	
cat <*file*>	Show the contents of a file
cd <*directory*>	Change the current directory to the specified directory
clrscrn	Clears the screen.
compact	Compact the file system, freeing all dirty space
cp <*source file*> <*destination file*>	Copy an existing file
dump <*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
ls	Show all files and directories in the current directory
ls <*directory*>	Show all files and directories in the specified directory
mkdir <*directory*>	Create a directory
mv <*source file*> <*destination file*>	Move a file on the file system
pwd	Print working directory
rm <*file*>	Remove a file

rmdir <*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 ascii <*source file*> <*destination file*> <*host*>	Get an ascii file using TFTP
tftp get ascii <*source file*> <*destination file*> <*host*> <*port*>	Get an ascii file using TFTP
tftp get binary <*source file*> <*destination file*> <*host*>	Get a binary file using TFTP
tftp get binary <*source file*> <*destination file*> <*host*> <*port*>	Get a binary file using TFTP
tftp put ascii <*source file*> <*destination file*> <*host*>	Put an ascii file using TFTP
tftp put ascii <*source file*> <*destination file*> <*host*> <*port*>	Put an ascii file using TFTP
tftp put binary <*source file*> <*destination file*> <*host*>	Put a binary file using TFTP
tftp put binary <*source file*> <*destination file*> <*host*> <*port*>	Put a binary file using TFTP
touch <*file*>	Create a file
ftp (config-ftp) level commands	
admin password <*text*>	Sets the administrative password for the FTP server. <text> = administrative password.
admin username <*text*>	Sets the administrative username for the FTP server. <text> = administrative username. It also removes the administrative password.
clear counters	Zeros FTP counters.
clrscrn	Clears the screen.
default admin username	Resets the FTP username to the default (admin).
exit	Returns to the config level.
no admin password	Removes the FTP administrative password.
no clear counters	Unzeros FTP counters.
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:2:1) 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.

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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.

protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.

ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:2:10) 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.
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
clrscrn	Clears the screen.
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 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>*	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 10 (tunnel-connect-host:1:10) 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.
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

clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:2:11) 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 punctuation: 123ABC "12 3A BC" 12,3A,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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:2:12) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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

	CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:2:13) 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.
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
clrscrn	Clears the screen.
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 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>*	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol 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*>	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 13 (tunnel-connect-host:1:13) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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 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.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:2:14) 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 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.
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-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*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 14 (tunnel-connect-host:1:14) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:2:15) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 (tunnel-connect-host:1:15) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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	
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.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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

	CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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>*	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol 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*>	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 16 (tunnel-connect-host:1:16) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 16 (config-host:16) 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.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:2:2) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 2 (tunnel-connect-host:1:2) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:2:3) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 3 (tunnel-connect-host:1:3) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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

	CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:2:4) 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.
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
clrscrn	Clears the screen.
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 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>*	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol 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*>	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 4 (tunnel-connect-host:1:4) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:2:5) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 5 (tunnel-connect-host:1:5) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:2:6) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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

	CLI session.
ssh 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:2:7) 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.
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
clrscrn	Clears the screen.
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 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>*	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.

protocol tcp aes	Uses TCP protocol 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*>	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 7 (tunnel-connect-host:1:7) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:2:8) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 8 (tunnel-connect-host:1:8) 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.
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
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 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
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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 CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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:1:9) 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.
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.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
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 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*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol 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*>	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 (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*>	Change to config host level
name <*text*>	Sets the name of the host. <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.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
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

	CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
http (config-http) level commands	
auth *<uri>* *<realm>*	Creates a new HTTP server authentication directive. <uri> = URI of the server. <realm> = domain of the server.
auth type *<uri>* basic	Sets an HTTP server authentication directive to the Basic Access Authentication scheme. <uri> = URI of the server.
auth type *<uri>* digest	Sets an HTTP server authentication directive to the Digest Access Authentication scheme. <uri> = URI of the server.
auth type *<uri>* none	Sets the authentication type for an HTTP server authentication directive to none. <uri> = URI of the server.
auth type *<uri>* ssl	Sets the authentication type for an HTTP server authentication directive to SSL. <uri> = URI of the server.
auth type *<uri>* ssl-basic	Sets the authentication type for an HTTP server authentication directive to SSL-Basic. <uri> = URI of the server.
auth type *<uri>* ssl-digest	Sets the authentication type for an HTTP server authentication directive to SSL-Digest. <uri> = URI of the server.
auth user *<uri>* *<user>* *<password>*	Creates or modifies a user for an HTTP server authentication directive. <uri> = URI of the server. <user> = username. <password> = password associated with the username.
authentication timeout *<minutes>*	For any Digest AuthType, sets the timeout for authentication. <minutes> = authentication timeout value.
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>*	Deletes an existing HTTP Server authentication directive. <uri> = URI of the server.

delete auth user <*uri*> <*user*>	Deletes an existing user for an HTTP Server authentication directive. <uri> = URI of the server. <user> = username.
exit	Returns to the config level.
log format <*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
logging state disable	Disables HTTP server logging.
logging state enable	Enables HTTP server logging.
max bytes <*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.
max timeout <*seconds*>	Sets the maximum time the HTTP server waits when receiving a request. <seconds> = maximum timeout value.
no clear counters	Restores the HTTP counters to the aggregate values.
no port	Disables the HTTP Server port.
no secure port	Disables the HTTP Server SSL port.
port <*number*>	Sets the port number the HTTP server will use. <number> = port number.
secure port <*number*>	Sets the port number the HTTP server will use over SSL. <number> = port 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	
auto show statistics	Continuously shows ICMP statistics
clear counters	Zeros counters
clrscrn	Clears the screen.
exit	Exits to the configuration level.
no clear counters	Unzeros IP counters
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Shows ICMP statistics
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>*	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
dhcp client id binary *<binary>*	Sets the client id allowing binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
dhcp client id set *<text>*	Sets the client id in text format.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
dhcp renew	Force DHCP to renew
domain *<text>*	Sets the domain name. <text> = name of the domain.
exit	Exits to the config level.
hostname *<text>*	Sets the host name. <text> = name of the host.
if *<instance>*	Changes to the interface configuration level.
ip address *<ip address/cidr>*	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>*	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>*	Sets the IP address of the primary DNS server.
secondary dns *<ip address>*	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:wlan0) level commands	
bootp disable	Disables BOOTP.
bootp enable	Enables BOOTP.
clrscrn	Clears the screen.
default gateway *<ip address>*	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
dhcp client id binary *<binary>*	Sets the client id allowing binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
dhcp client id set *<text>*	Sets the client id in text format.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
dhcp renew	Force DHCP to renew
domain *<text>*	Sets the domain name. <text> = name of the domain.
exit	Exits to the config level.
hostname *<text>*	Sets the host name. <text> = name of the host.
if *<instance>*	Changes to the interface configuration level.
ip address *<ip address/cidr>*	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>*	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>*	Sets the IP address of the primary DNS server.
secondary dns *<ip address>*	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	
auto show statistics	Continuously shows IP statistics
clear counters	Zeros counters
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*>	Sets the IP time to live, known by SNMP as "ipDefaultTTL". <hops> = number of hops that a typical IP packet is allowed to live.
multicast time to live <*hops*>	Sets the IP multicast time to live. <hops> = number of hops that a multicast IP packet is allowed to live.
no clear counters	Unzeros IP counters
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Shows IP statistics
write	Stores the current configuration in permanent memory.
ip filter (config-filter) level commands	
add <*ip address*> <*subnet mask*>	Adds an entry to the IP filter table.
clrscrn	Clears the screen.
exit	Returns to the config level.
no filtering	Removes filtering so ALL addresses are allowed.
remove <*ip address*> <*subnet mask*>	Removes an entry from the IP filter table.
show	Displays the IP filter table.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
key 1 (config-profile-security-wep-key:default_infrastructure_profile:1) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 1 (config-profile-security-wep-key:default_adhoc_profile:1) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 2 (config-profile-security-wep-key:default_infrastructure_profile:2) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 2 (config-profile-security-wep-key:default_adhoc_profile:2) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. 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.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 3 (config-profile-security-wep-key:default_infrastructure_profile:3) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. 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.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 3 (config-profile-security-wep-key:default_adhoc_profile:3) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. 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.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 4 (config-profile-security-wep-key:default_infrastructure_profile:4) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
key 4 (config-profile-security-wep-key:default_adhoc_profile:4) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
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.
line 1 (line:1) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <*bits per second*>	Sets the line speed. <bits 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 cp	Sets the current line to enter command mode under control of a CP.
command mode cp <*cp group*> <*value*>	Specifies the CP group and trigger value.
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*>	Sets a string that can be entered at boot time to enter command mode. <string> = text.
command mode serial string binary <*string*>	Sets a binary string that can be entered at boot time to enter command mode. <string> = string that may contain binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
command mode signon message <*string*>	Sets an ASCII sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text.
command mode signon message binary <*string*>	Sets a binary sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = string that may contain 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.
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 interface	Restores the default interface type to this line.
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*>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
interface rs232	Sets the line interface to RS232.
interface rs485 full-duplex	Sets the line interface to RS485 in full-duplex mode.
interface rs485 half-duplex	Sets the line interface to RS485 in half-duplex mode.

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.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
name <*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 cp	Disables control of a CP to enter command mode.
no command mode serial string	Prevents the user-defined serial boot string from being used to enter command mode in the CLI.
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.
ppp <*line*>	Enters the serial line PPP level.
protocol lpd	Applies Line Printer Daemon (LPD) protocol on the line.
protocol lpd or tunnel	Applies LPD or tunnel protocol on the line.
protocol modbus ascii	Applies Modbus ASCII protocol on the line.
protocol modbus rtu	Applies Modbus RTU protocol on the line.
protocol none	Uses no protocol on the line.
protocol ppp	Applies point-to-point protocol (PPP) 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*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <*bytes*>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.

write	Stores the current configuration in permanent memory.
xoff char <*control*>	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.
xon char <*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.
line 2 (line:2) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <*bits per second*>	Sets the line speed. <bits 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 cp	Sets the current line to enter command mode under control of a CP.
command mode cp <*cp group*> <*value*>	Specifies the CP group and trigger value.
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*>	Sets a string that can be entered at boot time to enter command mode. <string> = text.
command mode serial string binary <*string*>	Sets a binary string that can be entered at boot time to enter command mode. <string> = string that may contain binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
command mode signon message <*string*>	Sets an ASCII sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = text.
command mode signon message binary <*string*>	Sets a binary sign-on message that is sent from the serial port when the device boots and when the line is in command mode. <string> = string that may contain 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.
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 interface	Restores the default interface type to this line.
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*>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
interface rs232	Sets the line interface to RS232.
interface rs485 full-duplex	Sets the line interface to RS485 in full-duplex mode.
interface rs485 half-duplex	Sets the line interface to RS485 in half-duplex mode.
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.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
name <*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 cp	Disables control of a CP to enter command mode.
no command mode serial string	Prevents the user-defined serial boot string from being used to enter command mode in the CLI.
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.
ppp <*line*>	Enters the serial line PPP level.
protocol lpd	Applies Line Printer Daemon (LPD) protocol on the line.
protocol lpd or tunnel	Applies LPD or tunnel protocol on the line.
protocol modbus ascii	Applies Modbus ASCII protocol on the line.
protocol modbus rtu	Applies Modbus RTU protocol on the line.
protocol none	Uses no protocol on the line.
protocol ppp	Applies point-to-point protocol (PPP) 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*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
threshold <*bytes*>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <*control*>	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.
xon char <*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.
link (config-wlan:wlan0) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
choice <*instance*>	Enters the next lower level. Specify the instance for the next lower level.
clrscrn	Clears the screen.
default out of range scan interval	Restores the default value to the out-of-range scan interval (30 sec).
exit	Exit back to interface configuration level
out of range scan interval <*seconds*>	Sets the value of the out-of-range scan interval. <seconds> = Interval between scans when the device has deemed it is out of range of networks in its configuration. NOTE: Scans use more power than idling. The longer the interval the less power consumption. But also more possible detection latency when moving within range of a network.

roaming disable	Disables roaming.
roaming enable	Enables roaming to other Access Points with the same SSID.
scan	Scan the radio environment for all networks.
scan <*ssid*>	Scan the radio environment for the named network.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
status	Show link status
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 auto-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 auto	Sets 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	Disables log output.
default severity level	Log all events.
exit	Exits to the next higher level.
max length <*Kbytes*>	Sets the maximum size in Kbytes for the Log file.
output disable	Enables log to filesystem.
output filesystem	Enables log to serial line.
output line <*number*>	Could not find VarID 438 entry 3 in file http/config/varid_help.mtxt
severity level debug	Log all events.
severity level error	Log only Error and more severe events.
severity level information	Log only Information and more severe events.
severity level notice	Log only Notice and more severe events.
severity level warning	Log only Warning and more severe events.
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.
lpd (lpd) level commands	
auto show <*line*>	Continuously displays lpd status for the specified line. <line> = LPD line to display.

clrscrn	Clears the screen.
exit	Exits to the enable level.
kill <*line*>	Kills the current print job on the specified line. <line> = LPD line with print job.
show <*line*>	Displays lpd status for the specified line. <line> = LPD line to display.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
lpd 1 (config-lpd:1) level commands	
banner disable	Disables printing banner for all print jobs. Only print the banner when a job requests it.
banner enable	Enables printing banner for all print jobs.
binary disable	Treats print job as ascii text. Filters out all non-ascii characters and certain control characters.
binary enable	Treats print job as binary. Sends data byte-for-byte to the printer.
capture disable	Redirects serial output back to the line.
capture enable	Redirects serial output from the line to this CLI session.
clrscrn	Clears the screen.
convert newline disable	Disables converting single new line and carriage return characters to DOS-style line endings.
convert newline enable	Enables converting single new line and carriage return characters to DOS-style line endings. If characters are already in DOS line-ending order, they are not converted.
eoj disable	Disables sending the end-of-job string after each print job.
eoj enable	Enables sending the end-of-job string after each print job.
eoj text binary <*binary*>	Sets the end-of-job text allowing for binary characters. <binary> = string in binary format that will be sent to the printer at the end of each print job. Within [] use binary decimal up to 255 or hex up to 0xFF.
eoj text set <*text*>	Sets the end-of-job text. <text> = ascii string that will be sent to the printer at the end of each print job.
exit	Exits to the configuration level.
formfeed disable	Disables the printer from advancing to the next page at the end of each print job.
formfeed enable	Forces the printer to advance to the next page at the end of each print job.
kill	Ends the current print job on this lpd line.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
no eoj text	Removes the end-of-job string.

no queue name	Removes the queue name.
no soj text	Removes the start-of-job string.
ppp <*line*>	Enters the serial line PPP level.
queue name <*text*>	Sets the name of the queue that this lpd line belongs to. <text> = name for the queue.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays statistics and status information for this lpd line.
soj disable	Disables sending the start-of-job string after each print job.
soj enable	Enables sending the start-of-job string after each print job.
soj text binary <*binary*>	Sets the start-of-job text allowing for binary characters. <binary> = string in binary format that will be sent to the printer at the beginning of each print job. Within [] use binary decimal up to 255 or hex up to 0xFF.
soj text set <*text*>	Sets the start-of-job text. <text> = ascii string that will be sent to the printer at the beginning of each print job.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
test print <*number of lines*>	Prints lines of text directly to the lpd line. <number of lines> = number of lines to print.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
lpd 2 (config-lpd:2) level commands	
banner disable	Disables printing banner for all print jobs. Only print the banner when a job requests it.
banner enable	Enables printing banner for all print jobs.
binary disable	Treats print job as ascii text. Filters out all non-ascii characters and certain control characters.
binary enable	Treats print job as binary. Sends data byte-for-byte to the printer.
capture disable	Redirects serial output back to the line.
capture enable	Redirects serial output from the line to this CLI session.
clrscrn	Clears the screen.
convert newline disable	Disables converting single new line and carriage return characters to DOS-style line endings.
convert newline enable	Enables converting single new line and carriage return characters to DOS-style line endings. If characters are already in DOS line-ending order, they are not converted.
eoj disable	Disables sending the end-of-job string after each print job.
eoj enable	Enables sending the end-of-job string after each print job.

eoj text binary <*binary*>	Sets the end-of-job text allowing for binary characters. <binary> = string in binary format that will be sent to the printer at the end of each print job. Within [] use binary decimal up to 255 or hex up to 0xFF.
eoj text set <*text*>	Sets the end-of-job text. <text> = ascii string that will be sent to the printer at the end of each print job.
exit	Exits to the configuration level.
formfeed disable	Disables the printer from advancing to the next page at the end of each print job.
formfeed enable	Forces the printer to advance to the next page at the end of each print job.
kill	Ends the current print job on this lpd line.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be config-ured.
no eoj text	Removes the end-of-job string.
no queue name	Removes the queue name.
no soj text	Removes the start-of-job string.
ppp <*line*>	Enters the serial line PPP level.
queue name <*text*>	Sets the name of the queue that this lpd line belongs to. <text> = name for the queue.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays statistics and status information for this lpd line.
soj disable	Disables sending the start-of-job string after each print job.
soj enable	Enables sending the start-of-job string after each print job.
soj text binary <*binary*>	Sets the start-of-job text allowing for binary characters. <binary> = string in binary format that will be sent to the printer at the beginning of each print job. Within [] use binary decimal up to 255 or hex up to 0xFF.
soj text set <*text*>	Sets the start-of-job text. <text> = ascii string that will be sent to the printer at the beginning of each print job.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be con-figured.
terminal network	Enters the configure-terminal level for the network.
test print <*number of lines*>	Prints lines of text directly to the lpd line. <number of lines> = number of lines to print.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be con-figured.
write	Stores the current configuration in permanent memory.
modbus (modbus) level commands	

additional port *<number>*	Sets an additional TCP server port.
clrscrn	Clears the screen.
default response timeout	Restores the default Modbus Response Timeout.
exit	Exits to the config level.
kill connection *<index>*	Kills modbus connection selected by index from show connections.
no additional port	Removes the additional TCP server port.
response timeout *<milliseconds>*	Sets the Modbus Response Timeout in milliseconds.
rss	Enters the next lower level.
show	Displays the current configuration.
show connections	Displays connections.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays statistics.
tcp server state disable	Disables the Modbus TCP Server.
tcp server state enable	Enables the Modbus TCP Server.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:2) 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.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.

verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:1) level commands	
clrscrn	Clears the screen.
connect string *<text>*	Sets the CONNECT string used in modem emulation. <string> = connect 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.
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*>	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.
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. <bytes> = number of bytes in the threshold.
timeout <*milliseconds*>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.
trailing character <*control*>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:1) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <*control*>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <*bytes*>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <bytes> = number of bytes in the threshold.
timeout <*milliseconds*>	Sets the timeout value for packing mode in milliseconds.

	<milliseconds> = timeout value, in milliseconds.
trailing character <*control*>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:2) 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*>	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:1) 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*>	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.
ppp 1 (ppp:1) level commands	
authentication mode chap	Sets authentication to Challenge-Handshake Authentication Protocol (CHAP).
authentication mode ms-chap	Sets authentication to MS-CHAP version 1.
authentication mode ms-chapv2	Sets authentication to MS-CHAP version 2.
authentication mode none	Removes PPP authentication.
authentication mode pap	Sets authentication to Password Authentication Protocol (PAP).
clrscrn	Clears the screen.
default authentication mode	Removes PPP authentication.

exit	Exits to the configuration level.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
local ip <*ip address/cidr*>	Sets the Local 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)
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
no local ip	Removes the Local IP address.
no password	Removes the PPP authentication password.
no peer ip	Removes the peer IP address.
no username	Removes the PPP authentication username.
password <*text*>	Sets the password for PPP authentication.
peer ip <*ip address*>	Sets the IP Address assigned to the peer when requested during negotiation. <ip address> IP address of the peer device.
ppp <*line*>	Enters the serial line PPP level.
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. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
username <*text*>	Sets the user name for PPP authentication.
write	Stores the current configuration in permanent memory.
ppp 2 (ppp:2) level commands	
authentication mode chap	Sets authentication to Challenge-Handshake Authentication Protocol (CHAP).
authentication mode ms-chap	Sets authentication to MS-CHAP version 1.
authentication mode ms-chapv2	Sets authentication to MS-CHAP version 2.
authentication mode none	Removes PPP authentication.
authentication mode pap	Sets authentication to Password Authentication Protocol (PAP).
clrscrn	Clears the screen.
default authentication mode	Removes PPP authentication.
exit	Exits to the configuration level.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
local ip <*ip address/cidr*>	Sets the Local 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)
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.

no local ip	Removes the Local IP address.
no password	Removes the PPP authentication password.
no peer ip	Removes the peer IP address.
no username	Removes the PPP authentication username.
password <*text*>	Sets the password for PPP authentication.
peer ip <*ip address*>	Sets the IP Address assigned to the peer when requested during negotiation. <ip address> IP address of the peer device.
ppp <*line*>	Enters the serial line PPP level.
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. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
username <*text*>	Sets the user name for PPP authentication.
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*>	Ping destination continuously with 5 second timeout
ping <*host*> <*count*>	Ping destination n times with 5 second timeout
ping <*host*> <*count*> <*timeout*>	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 matchport_bg_pro	Show system information
trace route <*host*>	Trace route to destination
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*>	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.
rss (modbus-rss) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
trace input disable	Disables RSS trace of Modbus PDUs received on the serial line.
trace input enable	Enables RSS trace of Modbus PDUs received on the serial line.
write	Stores the current configuration in permanent memory.
security (config-profile-security:default_infrastructure_profile) level commands	
advanced	Switch to advanced level
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
basic	Switch to basic level
clrscrn	Clears the screen.
default key type	Restores the key type to the default value (passphrase).
default suite	Restores the security method (suite) to the default value (None).
exit	Exit to the profiles level
key type hex	Sets the key type to hex.
key type passphrase	Sets the key type to passphrase.
no passphrase	Removes the passphrase.
passphrase <*text*>	Sets the passphrase. Maximum 63 characters. <text> = put quotes around characters that make up the passphrase. Please refer to the other equipment's manual to determine the passphrase input style recommended. NOTE: Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
suite none	Sets the security suite to None.
suite wep	Sets the security suite to WEP.
suite wpa	Sets the security suite to WPA.
suite wpa2	Sets the security suite to WPA2.
wep	Enters the next lower level.

wpax	Enters the next lower level.
write	Stores the current configuration in permanent memory.
security (config-profile-security:default_adhoc_profile) level commands	
advanced	Switch to advanced level
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
basic	Switch to basic level
clrscrn	Clears the screen.
default key type	Restores the key type to the default value (passphrase).
default suite	Restores the security method (suite) to the default value (None).
exit	Exit to the profiles level
key type hex	Sets the key type to hex.
key type passphrase	Sets the key type to passphrase.
no passphrase	Removes the passphrase.
passphrase <*text*>	Sets the passphrase. Maximum 63 characters. <text> = put quotes around characters that make up the passphrase. Please refer to the other equipment's manual to determine the passphrase input style recommended. NOTE: Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
suite none	Sets the security suite to None.
suite wep	Sets the security suite to WEP.
suite wpa	Sets the security suite to WPA.
suite wpa2	Sets the security suite to WPA2.
wep	Enters the next lower level.
wpax	Enters the next lower level.
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*>	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*>	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*>	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*>	Sets an SMTP relay address to direct all outbound email messages through a mail server.
relay port <*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.

snmp (config-snmp) level commands	
clrscrn	Clears the screen.
default read community	Clears the SNMP read-only community.
default system description	Restores the SNMP system description to its default.
default system name	Restores the SNMP system name to default: the product name.
default write community	Clears the SNMP read/write community.
exit	Returns to the config level.
no system contact	Clears the SNMP system contact.
no system location	Clears the SNMP system location.
read community <*text*>	Sets the SNMP read-only community string. <text> = name of the read-only community string to be set.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays the SNMP agent status.
state disable	Disables the SNMP server.
state enable	Enables the SNMP server.
system contact <*text*>	Sets the SNMP system contact information. <text> = system contact information.
system description <*text*>	Sets the SNMP system description. <text> = description of device.
system location <*text*>	Sets the SNMP system location. <text> = location of device.
system name <*text*>	Sets the SNMP system name. <text> = SNMP system name.
traps	Enters the next lower level.
write	Stores the current configuration in permanent memory.
write community <*text*>	Sets the SNMP read-write community string. <text> = name of the read-write community string to be set.
ssh (ssh) level commands	
client	Enters the SSH Client configuration level.
clrscrn	Clears the screen.
exit	Exits to the enable level.
server	Enters the SSH Server configuration level.
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	
clear counters	Sets the SSH counters to zero.
clrscrn	Clears the screen.
default max sessions	Could not find VarID 316 in file http/config/varid_help.mtxt
default port	Restores the default local port to the SSH server.
exit	Exits to the CLI level.
max sessions <*number*>	Could not find VarID 316 in file http/config/varid_help.mtxt
no clear counters	Restores the SSH counters to the aggregate values.
port <*number*>	Sets the local port that the SSH server uses. <number> = local port 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	
authority	Adds an Authority Certificate.
clrscrn	Clears the screen.
dsa	Adds DSA Certificate and Private Key.
exit	Exits to the enable level.
generate dsa	Generates a new Self-Signed DSA Certificate.
generate rsa	Generates a new Self-Signed RSA Certificate.
no dsa	Removes DSA Certificate and Private Key
no intermediate authority *<cert>*	Removes an Intermediate Authority Certificate. <cert> = index displayed by "show authority" command.
no rsa	Removes RSA Certificate and Private Key
no trusted authority *<cert>*	Removes a Trusted Authority Certificate. <cert> = index displayed by "show authority" command.
rsa	Adds RSA Certificate and Private Key.
show	Displays Certificate Information.
show authority	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.
syslog (config-syslog) level commands	
clrscrn	Clears the screen.
default local port	Restores the default syslog local port.
default remote port	Restores the default syslog remote port.
default severity log level	No logging.
exit	Returns to the config level.
host *<text>*	Sets the address of the syslog recipient. <text> = IP address or name of the host.
local port *<number>*	Sets the syslog local port. <number> = number of the local port used when making a syslog connection.
no host	Removes the address of the syslog recipient.
remote port *<number>*	Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.
severity log level alert	Log only Alert and more severe events.
severity log level critical	Log only Critical and more severe events.
severity log level debug	Log all events.
severity log level emergency	Log only Emergency events.
severity log level error	Log only Error and more severe events.
severity log level information	Log only Information and more severe events.
severity log level none	No logging.
severity log level notice	Log only Notice and more severe events.
severity log level warning	Log only Warning and more severe events.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the syslog statistics.
state disable	Disables syslog logging.
state enable	Enables syslog logging.
write	Stores the current configuration in permanent memory.
tcp (config-tcp) level commands	
ack limit <*packets*>	Sets the number of packets that must be received before an ACK is forced. If there is a large amount of data to acknowledge, an ACK will be forced before this.
auto show statistics	Continuously shows TCP statistics
clear counters	Zeros TCP counters
clrscrn	Clears the screen.
default ack limit	Restores the default ack limit of 3 packets.
default max retrans	Restores the default Maximum Retransmissions.
default max retrans syn ack	Restores the default Maximum Retransmissions for SYN/ACK.
default max timeout	Restores the default Maximum Timeout between retrans-missions.
default send data	Sets TCP to send data in accordance with standards.
exit	Exits to the configuration level.
max retrans <*number*>	Sets the Maximum Retransmisssions.
max retrans syn ack <*number*>	Sets the Maximum Retransmisssions for SYN/ACK. It is lower than "Max Retrans" to thwart denial-of-service attacks.
max timeout <*seconds*>	Sets the Maximum Timeout between retransmisssions in seconds.
no clear counters	Unzeros TCP counters
resets disable	Does not send TCP RSTs upon connection to unused ports.
resets enable	Sends TCP RSTs upon connection to unused ports.
send data expedited	Sets TCP to send data whenever the window is sufficient-ly open, for improved real-time performance.
send data standard	Sets TCP to send data in accordance with standards.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Shows TCP statistics
write	Stores the current configuration in permanent memory.
telnet (config-cli-telnet) level commands	
clear counters	Sets the Telnet counters to zero.
clrscrn	Clears the screen.
default max sessions	Could not find VarID 315 in file http/config/varid_help.mtxt
default port	Restores the default local port to the Telnet server.
exit	Exits to the CLI level.
max sessions <*number*>	Could not find VarID 315 in file http/config/varid_help.mtxt
no clear counters	Restores the Telnet counters to the aggregate values.
port <*number*>	Sets the local port that the Telnet server uses.

	<number> = local port 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*>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of 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*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
no send break	Removes the configured send break character.
ppp <*line*>	Enters the serial line PPP level.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*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.
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. <line> = number of the terminal line (serial port) to be configured.

terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 2 (config-terminal:2) level commands	
break duration <*milliseconds*>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of 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*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
no send break	Removes the configured send break character.
ppp <*line*>	Enters the serial line PPP level.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*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.
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. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.

tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal network (config-terminal:network) level commands	
break duration <*milliseconds*>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of 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*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
lpd <*line*>	Enters the configure lpd level. <line> = number of the line (lpd serial port) to be configured.
no send break	Removes the configured send break character.
ppp <*line*>	Enters the serial line PPP level.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*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.
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. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be con-

	figured.
write	Stores the current configuration in permanent memory.
tftp (config-tftp) level commands	
allow file creation disable	Prohibits the TFTP server from creating files on the file system.
allow file creation enable	Enables the TFTP server to create files on the file system.
allow firmware update disable	The TFTP server rejects any attempt to update firmware.
allow firmware update enable	The TFTP server accepts a firmware image for update based on the file name.
allow xcr import disable	The TFTP server rejects any attempt to import XML configuration.
allow xcr import enable	The TFTP server accepts an XCR file for configuration update based on the file name.
clear counters	Sets the TFTP counters to zero.
clrscrn	Clears the screen.
exit	Returns to the config level.
no clear counters	Restores the TFTP counters to the aggregate values.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the TFTP statistics.
state disable	Disables the TFTP server.
state enable	Enables the TFTP server.
write	Stores the current configuration in permanent memory.
traps (config-snmp-traps) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no primary destination	Deletes the primary SNMP trap host.
no secondary destination	Deletes the secondary SNMP trap host.
primary destination <*text*>	Sets the primary SNMP trap host. <text> = IP address of host running the SNMP trap.
secondary destination <*text*>	Sets the secondary SNMP trap host. <text> = IP address of host running the SNMP trap.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables the sending of SNMP trap messages.
state enable	Enables the sending of SNMP trap messages.
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*>	Enters the line level. <line> = number of the line (serial port) to be configured.
lpd <*line*>	Enters the configure lpd level.

	<line> = number of the line (lpd 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.
ppp *<line>*	Enters the serial line PPP level.
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. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel *<line>*	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
tunnel 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. <line> = number of the line (serial port) to be configured.
lpd *<line>*	Enters the configure lpd level. <line> = number of the line (lpd 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.
ppp *<line>*	Enters the serial line PPP level.
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. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel *<line>*	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
udp (config-udp) level commands	
auto show statistics	Continuously shows UDP statistics
clear counters	Zeros counters
clrscrn	Clears the screen.

exit	Exits to the configuration level.
no clear counters	Unzeros IP counters
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Shows UDP statistics
write	Stores the current configuration in permanent memory.
verbosity (config-diagnostics-verbosity) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
wlan	Enters the next lower level.
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.
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.
wep (config-profile-security-wep:default_infrastructure_profile) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
authentication open	Sets the type of authentication to open.
authentication shared	Sets the type of authentication to shared.
clrscrn	Clears the screen.
default authentication	Restores the authentication type to the default value (open).
default key size	Restores the key size to the default value (40 bits).
default tx key index	Restores the tx key index to the default value (1).
exit	Exits to the next higher level.
key *<instance>*	Enters the next lower level. Specify the instance for the next lower level.
key size 104	Sets the key size to 104 bits.
key size 40	Sets the key size to 40 bits.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
tx key index 1	Selects key 1 for transmission encryption.

tx key index 2	Selects key 2 for transmission encryption.
tx key index 3	Selects key 3 for transmission encryption.
tx key index 4	Selects key 4 for transmission encryption.
write	Stores the current configuration in permanent memory.
wep (config-profile-security-wep:default_adhoc_profile) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
authentication open	Sets the type of authentication to open.
authentication shared	Sets the type of authentication to shared.
clrscrn	Clears the screen.
default authentication	Restores the authentication type to the default value (open).
default key size	Restores the key size to the default value (40 bits).
default tx key index	Restores the tx key index to the default value (1).
exit	Exits to the next higher level.
key *<instance>*	Enters the next lower level. Specify the instance for the next lower level.
key size 104	Sets the key size to 104 bits.
key size 40	Sets the key size to 40 bits.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
tx key index 1	Selects key 1 for transmission encryption.
tx key index 2	Selects key 2 for transmission encryption.
tx key index 3	Selects key 3 for transmission encryption.
tx key index 4	Selects key 4 for transmission encryption.
write	Stores the current configuration in permanent memory.
wlan (config-diagnostics-verbosity-wlan) level commands	
clrscrn	Clears the screen.
default detail	Sets the WLAN verbosity detail to its default value, Minimum.
default topic	Restores the WLAN verbosity topics to the default value (none enabled).
detail everything	Sets the WLAN verbosity detail to Everything.
detail intermediate	Sets the WLAN verbosity detail to Intermediate.
detail minimum	Sets the WLAN verbosity detail to Minimum.
exit	Exits to the next higher level.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
topic assoc disable	Disables this WLAN verbosity topic.
topic assoc enable	Enables this WLAN verbosity topic.
topic cmd disable	Disables this WLAN verbosity topic.
topic cmd enable	Enables this WLAN verbosity topic.
topic dwnld disable	Disables this WLAN verbosity topic.
topic dwnld enable	Enables this WLAN verbosity topic.
topic event disable	Disables this WLAN verbosity topic.
topic event enable	Enables this WLAN verbosity topic.

topic init disable	Disables this WLAN verbosity topic.
topic init enable	Enables this WLAN verbosity topic.
topic ioctl disable	Disables this WLAN verbosity topic.
topic ioctl enable	Enables this WLAN verbosity topic.
topic proc disable	Disables this WLAN verbosity topic.
topic proc enable	Enables this WLAN verbosity topic.
topic pwsv disable	Disables this WLAN verbosity topic.
topic pwsv enable	Enables this WLAN verbosity topic.
topic rx disable	Disables this WLAN verbosity topic.
topic rx enable	Enables this WLAN verbosity topic.
topic scan disable	Disables this WLAN verbosity topic.
topic scan enable	Enables this WLAN verbosity topic.
topic tx disable	Disables this WLAN verbosity topic.
topic tx enable	Enables this WLAN verbosity topic.
write	Stores the current configuration in permanent memory.
wlan profiles (config-profiles) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
create <*profile name*>	Create a new profile name
delete <*profile name*>	Delete existing profile by name
edit <*profile name*>	View or edit an existing profile
exit	Exits to the config level.
show	Show existing profile names
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
wpax (config-profile-security-wpax:default_infrastructure_profile) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
authentication 802.1x	Sets the authentication method to IEEE 802.1x.
authentication psk	Sets the authentication method to PSK.
clrscrn	Clears the screen.
default authentication	Restores the authentication method to the default value (PSK).
default eap-ttls option	Restores the eap-ttls protocol options to the default (EAP-MSCHAP V2).
default encryption	Restores the encryption type to the default value (none enabled).
default ieee 802.1x	Restores the default IEEE 802.1x protocol, EAP-TTLS.
default peap option	Restores the PEAP authentication protocol options to the default (EAP-MSCHAP V2).
eap-ttls option chap	Sets the EAP-TTLS authentication protocol option to CHAP.
eap-ttls option eap-md5	Sets the EAP-TTLS authentication protocol option to EAP-MD5.
eap-ttls option eap-mschapv2	Sets the EAP-TTLS authentication protocol option to EAP-MSCHAP V2.

eap-ttls option mschap	Sets the EAP-TTLS authentication protocol option to MSCHAP.
eap-ttls option mschapv2	Sets the EAP-TTLS authentication protocol option to MSCHAP V2.
eap-ttls option pap	Sets the EAP-TTLS authentication protocol option to PAP.
encryption ccmp disable	Disables this encryption method.
encryption ccmp enable	Enables this encryption method.
encryption tkip disable	Disables this encryption method.
encryption tkip enable	Enables this encryption method.
encryption wep disable	Disables this encryption method.
encryption wep enable	Enables this encryption method.
exit	Exits to the next higher level.
ieee 802.1x eap-tls	Sets the IEEE 802.1x protocol to EAP-TLS.
ieee 802.1x eap-ttls	Sets the IEEE 802.1x protocol to EAP-TTLS.
ieee 802.1x leap	Sets the IEEE 802.1x protocol to LEAP.
ieee 802.1x peap	Sets the IEEE 802.1x protocol to PEAP.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
no password	Clears the password.
no username	Clears the user name.
password <*text*>	Sets the value for the password. <text> = put quotes around the characters (max 63).
peap option eap-md5	Sets the PEAP authentication protocol option to EAP-MD5.
peap option eap-mschapv2	Sets the PEAP authentication protocol option to EAP-MSCHAP V2.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <*text*>	Sets the value of the username. <text> = value in characters (max 63).
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
wpax (config-profile-security-wpax:default_adhoc_profile) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
authentication 802.1x	Sets the authentication method to IEEE 802.1x.
authentication psk	Sets the authentication method to PSK.

clrscrn	Clears the screen.
default authentication	Restores the authentication method to the default value (PSK).
default eap-ttls option	Restores the eap-ttls protocol options to the default (EAP-MSCHAP V2).
default encryption	Restores the encryption type to the default value (none enabled).
default ieee 802.1x	Restores the default IEEE 802.1x protocol, EAP-TTLS.
default peap option	Restores the PEAP authentication protocol options to the default (EAP-MSCHAP V2).
eap-ttls option chap	Sets the EAP-TTLS authentication protocol option to CHAP.
eap-ttls option eap-md5	Sets the EAP-TTLS authentication protocol option to EAP-MD5.
eap-ttls option eap-mschapv2	Sets the EAP-TTLS authentication protocol option to EAP-MSCHAP V2.
eap-ttls option mschap	Sets the EAP-TTLS authentication protocol option to MSCHAP.
eap-ttls option mschapv2	Sets the EAP-TTLS authentication protocol option to MSCHAP V2.
eap-ttls option pap	Sets the EAP-TTLS authentication protocol option to PAP.
encryption ccmp disable	Disables this encryption method.
encryption ccmp enable	Enables this encryption method.
encryption tkip disable	Disables this encryption method.
encryption tkip enable	Enables this encryption method.
encryption wep disable	Disables this encryption method.
encryption wep enable	Enables this encryption method.
exit	Exits to the next higher level.
ieee 802.1x eap-tls	Sets the IEEE 802.1x protocol to EAP-TLS.
ieee 802.1x eap-ttls	Sets the IEEE 802.1x protocol to EAP-TTLS.
ieee 802.1x leap	Sets the IEEE 802.1x protocol to LEAP.
ieee 802.1x peap	Sets the IEEE 802.1x protocol to PEAP.
key <*hexadecimal*>	Sets key. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
key text <*text*>	Sets key. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
no key	Removes key.
no password	Clears the password.
no username	Clears the user name.
password <*text*>	Sets the value for the password. <text> = put quotes around the characters (max 63).
peap option eap-md5	Sets the PEAP authentication protocol option to EAP-MD5.
peap option eap-mschapv2	Sets the PEAP authentication protocol option to EAP-MSCHAP V2.

show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
username <*text*>	Sets the value of the username. <text> = value in characters (max 63).
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
write	Stores the current configuration in permanent memory.
xml (xml) level commands	
auto show statistics	Show XML statistics
clear counters	Zeros XML statistics
clrscrn	Clears the screen.
exit	Exits to the enable level.
no clear counters	Unzeros XML statistics
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*>	Save XML configuration containing secrets to a file
secret xcr export <*file*> <*group list*>	Save specified XML configuration containing secrets to a local file
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Show XML statistics
write	Stores the current configuration in permanent memory.
xcr dump	Dump XML configuration to the console
xcr dump <*group list*>	Dump specified XML configuration to the console
xcr export <*file*>	Save XML configuration to a file
xcr export <*file*> <*group list*>	Save specified XML configuration to a local file
xcr import <*file*>	Load XML configuration from a local file
xcr import <*file*> <*group list*>	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 <*group list*>	Dump specified XML Status Records to the console
xsr export <*file*>	Save XML Status Record to a file
xsr export <*file*> <*group list*>	Save specified XML Status Record to a local file
xsr list	List XML Status Record groups to the console