LANTRONIX®

MatchPort™
AR ARCHITECT

MatchPort AR Command Reference

Part Number 900-502
Revision C May 2010

Copyright and Trademark

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, and Windows NT are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation.

Warranty

For details on the Lantronix warranty replacement policy, please go to our web site at www.lantronix.com/support/warranty.

Contacts

Lantronix 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, correcponding to release 1.1.0.0.R6.
May 2010	C	Updated for firmware release 5.1.0.0R10.

Table of Contents

List of Figures

List of Tables

1: About This Guide

This guide describes how to configure the Lantronix Evolution OS™ for the MatchPort AR. You can use the Lantronix Evolution OS™ Web Manager, Command Line Interface (CLI), and/or Extensible Markup Language (XML). It is written for software developers and system integrators.

This chapter contains the following sections:

Chapter Summaries

Table 1-1 lists and summarizes each chapter.

Table 1-1 Chapters and Summaries

Chapter	Summary
2: Overview	Gives an overview of CLI and XML.
3: Configuration Using Command Line Interface	Lists commands and describes how to use CLI to configure the MatchPort AR.
4: Configuration Using XML	Describes configuration process using XML.
5: XML Configuration Groups	Lists XCR and XSR groups and items.

Conventions

Table 1-2 lists and describes the conventions used in this book.

Table 1-2 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.*

Table 1-2 Conventions Used in This Book (continued)

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.

- ***MatchPort AR User Guide***—Describes how to configure and use the MatchPort AR.
- ***MatchPort AR Integration Guide***—Contains information about the MatchPort AR hardware, the MatchPort AR demonstration board, and integrating the MatchPort AR into your product.
- ***MatchPort AR Demo Kit Quick Start Guide***—Describes how to get the MatchPort AR demonstration board up and running.

2: Overview

Evolution OS™ 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 AR User Guide* at the Lantronix website.

This chapter contains the following sections:

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.

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 a standard text editor or an XML editor.

For a brief overview of XML, see 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.

3: Configuration Using Command Line Interface

This chapter describes accessing the MatchPort AR command line interface (CLI) by using Telnet, SSH, or serial ports to configure the MatchPort AR. It also describes navigating the CLI, typing keyboard shortcuts, and moving between the levels.

It contains the following sections:

- Understanding the CLI Level Hierarchy
- Accessing the CLI via Telnet
- Accessing the CLI via Serial Ports
- Using Keyboard Shortcuts and CLI

Refer to the MatchPort AR Commands chapter for a complete list of levels, commands, and descriptions.

Understanding the CLI Level Hierarchy

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

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

Commands at the login level, shown in Figure 3-1, do not affect current configuration settings and are not displayed initially. If you type <**?**>, you will see the login–level sub–commands. These commands provide diagnostic and status information only.

Figure 3-1 Login Level Commands

```
>login

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

>
```

More device information and configuration options can be accessed via the enable level. The enable level is shown in Figure 3-2. The enable level can also be password protected and is the gateway to full configuration and management of the device server.

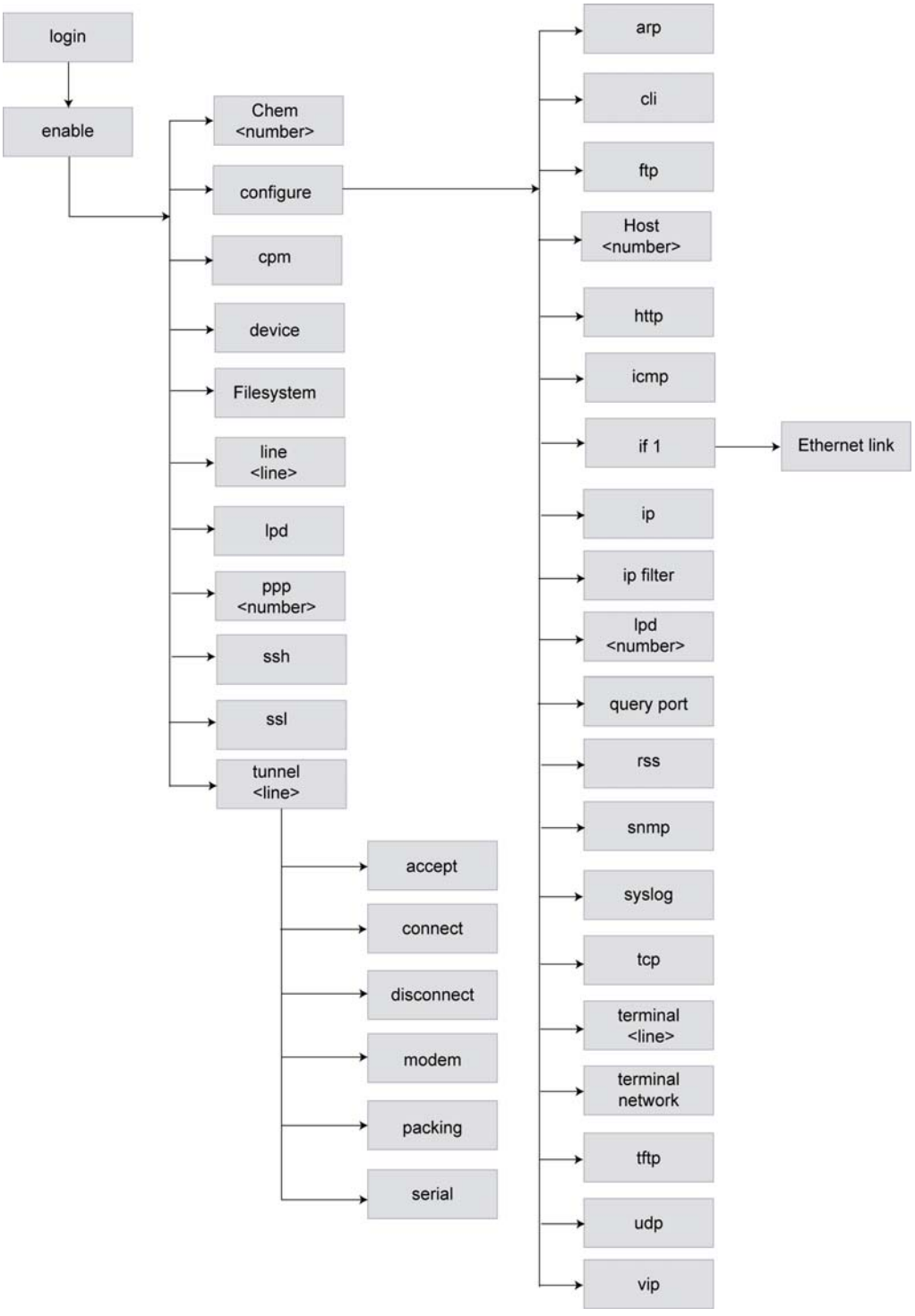
There are commands for gathering and effecting all elements of device status and configuration, as well as commands that take you to additional levels. For instance, tunnel specific status and configuration is found under the "tunnel" level, and network specific status and configuration commands are found under the "configuration" level.

Figure 3-2 Enable Level Commands

```
>enable
(enable)#?
auto show interfaces                        auto show processes
auto show xsr                               chem (number)
clear interfaces counters                   clear query port counters
clear xsr counters                          clrscrn
configure                                   connect
connect line (line)                         device
disable                                     exit
filesystem                                  kill line (line)
kill ssh (session)                          kill telnet (session)
line (line)                                 lpd
no clear interfaces counters                no clear query port counters
no clear xsr counters                       nslookup
nslookup (host)                             ping (host)
ping (host) (count)                         ping (host) (count) (timeout)
ppp (line)                                  reload
reload factory defaults                     secret xcr dump
secret xcr dump (group list)                secret xcr export (file)
secret xcr export (file) (group list)       show
show hello                                  show history
show hosts                                  show interfaces
show ip sockets                             show processes
show sessions                               show xsr
ssh                                         ssh (optClientUsername) (host)
ssh (optClientUsername) (host) (port)       ssl
telnet (host)                               telnet (host) (port)
trace route (host)                          tunnel (line)
write                                       xcr dump
xcr dump (group list)                       xcr export (file)
xcr export (file) (group list)              xcr import (file)
xcr import (file) (group list)              xcr list
xsr dump                                    xsr dump (group list)
xsr export (file)                           xsr export (file) (group list)
xsr list
```

An overview of the CLI levels and commands in the MatchPort AR are presented in Figure 3-3.

Figure 3-3 CLI Level Hierarchy



Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of levels. Each hierarchical level has a group of commands for a specific purpose. For example, to configure a setting for the FTP server, you would navigate to the FTP level by typing **enable > configure > ftp**. Navigating the CLI involves a few commands that are described in the following list.

- 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>#.
- 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.
- View the current configuration at any level—Type **show** and press the Enter key.
- View the list of commands available at the current level—Type the question mark "**?**" and press the Enter key. Items within < > (e.g. <string>) are required parameters.
- View the available commands and explanations—Type the asterisk (*****) and press the Enter key.
- View the list of commands available for a partial command—Type the partial command followed by the question mark "**?**" and press the Enter key. For example: <tunnel-1>#**echo?** displays a list of all echo commands at the tunnel level.
- View available commands and their explanations for a partial command—Type the partial command followed by the asterisk (*****) and press the Enter key. For example: <tunnel-1>#**echo*** displays a list of all echo commands and descriptions at the tunnel level.
- View the last 20 commands entered at the CLI—Type **show history** and press the Enter key.

Accessing the CLI via 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 User Guide* for more information.

To access the MatchPort AR by using Telnet, perform the following steps.

1. Click **Start > Run**. The **Run** dialog box displays.
2. Type telnet x.x.x.x (x.x.x.x is the IP address). The MatchPort AR is online when the command prompt (>) displays.
3. Enter the configuration CLI.

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

Accessing the CLI via 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 backdoor 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. The exclamation point displays on the terminal or PC screen.
4. Type xyz within 5 seconds to display the CLI prompt.

Using Keyboard Shortcuts and CLI

One useful shortcut built into Evolution OS™ 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. The first few characters of a command, the 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 by 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

To configure the MatchPort AR you must be in the enable level and any of its sub-levels. See the MatchPort AR Commands chapter at the end of this document for a complete list of levels, commands, and descriptions.

4: Configuration Using XML

The 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+)>
<!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 AR 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 serial string”>
         <value>disable</value>
      </configitem>
   </configgroup>
</configrecord>
```

The Evolution OS™ 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.

Name and Instance Attributes

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 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”>
      </configitem>
      <configitem name = “from”>
      </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 Record

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 AR 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_ar.xcr is requested. On export (FTP get of matchport_ar.xcr), the FTP server obtains the current XCR from Evolution OS™ and sends it as a file. On import (FTP put of matchport_ar.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_ar.xcr is not read from or written to the file system. See FTP in the *MatchPort AR User Guide*.
- TFTP—TFTP supports XCR importing. Due to limited security capabilities of TFTP, the option is disabled by default.

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.

Note: *Using Microsoft Word to edit and save an XCR will change the format of the file and make it incompatible with Evoltuion 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.

Note: *The filename matchport_ar.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_ar.xsr is not acceptable, because performing an FTP get on that name produces the current status and does not retrieve the file 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>
```

5: XML Configuration Groups

This chapter lists the MatchPort AR XML Configuration Record (XCR) groups and the XML Status Record (XSR) groups. It contains the following sections:

XCR Import and Export Groups

Table 5-1 lists and describes the MatchPort AR XCR groups in alphabetical order.

Table 5-1 XCR Import and Export Groups

Group: Subgroup Name	Item Name	Value Name	Value	Description
arp	arp entry	ip address		Adds a dynamic entry to the ARP table.
		mac address		
	arp delete	ip address		Removes an entry from the ARP table. Specify the entry by its IP address.
	timeout			In seconds.
cli	enable level password			If configured and not exporting secrets, exports only a placeholder.
	inactivity timeout			In minutes.
	login password			If configured and not exporting secrets, exports only a placeholder.
	quit connect line			Normally this will be a control key. For example, <control>L.
cp group	cp	bit		
		type		
		assert low		
	state		enable	
			disable	
device	firmware version			
	long name			
	serial number			
	short name			

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
email	cc			Multiple cc addresses may be separated with semicolons.
	cp	group		
		trigger value		
	from			
	local port			Either a specific number or “Random”.
	message file			
	overriding domain			
	priority		Very Low	
			Low	
			Normal	
			High	
			Urgent	
	reply to			
	subject			
	server port			
	to			Multiple to addresses may be separated with semicolons.
ethernet	duplex		auto	
			full	
			half	
	speed		auto	
			10	
			100	
			disable	
ftp server	admin username			
	admin password			If configured and not exporting secrets, exports only a placeholder.
	state		enable	
			disable	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
host	name			
	protocol		telnet	
			ssh	
	remote address			
	remote port			
	ssh username			Username must correspond to a configured ssh client user.
http authentication uri	realm		config	
			digest	
	type			
	user	password		If configured and not exporting secrets, exports only a placeholder.
	user delete	name		Deletes an HTTP Authentication URI user. The value element is used to specify the user for deletion.
http server	log format			
	logging state		enable	
			disable	
	max bytes			
	max log entries			
	max timeout			
	port			
	secure port			
	secure protocols	ssl3	enable	
			disable	
		ttls1.0	enable	
			disable	
		ttls1.1	enable	
			disable	
	state		enable	
			disable	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
icmp	state		enable	
			disable	
interface	bootp		enable	
			disable	
	default gateway			
	dhcp		enable	
			disable	
	dhcp client id			Set the identity of the client device.
	domain			
	hostname			
	ip address			Specifies both the address and mask.Use Classless Inter-Domain Routing (CIDR) form (192.168.0.1/16) or explicit mask (192.168.0.1 255.255.0.0)
	primary dns			
	secondary dns			
ip	multicast time to live			Specifies number of hops.
ip filter	delete entries		enable	Deletes any existing entries before adding “filter entry”.
			disable	
	filter delete	ip address		Deletes a specific IP filter entry.
		net mask		
	filter entry	ip address		
		net mask		
line	baud rate			Any value from 300 to 921600.
	data bits		8	
	flow control		software	
			none	
			hardware	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	gap timer			
	interface		rs485 half-duplex	
			rs485 full-duplex	
			rs232	
	name			
	parity		even	
			odd	
			none	
	protocol		lpd or tunnel	
			none	
			ppp	
			tunnel	
			lpd	
	state		enable	
			disable	
	stop bits		1	
			2	
	threshold			
	xon char			Set the x-on character. Prefix hex with 0x (0x11) or decimal with \(\17).
	xoff char			Set the x-off character. Prefix hex with 0x (0x11) or decimal with \(\17).
lpd	banner		enable	
			disable	
	binary		enable	
			disable	
	convert newline		enable	
			disable	
	eoj		disable	
			enable	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	eoj text			
	formfeed		disable	
			enable	
	queue name			
	soj		disable	
			enable	
	soj text			
managelinx	encrypted dsm credentials	dna.dsc.auth. tunnel. username		
		dna.dsc.auth. ssh.pub		
		dna.dsc.auth. ssh.priv		
		device.dna.dsc. tunnel.portlist. list		
		device.dna.dsc. tunnel.ip.addr		
		device.dna.dsc. tunnel.ssh. public		
		device.dnaid		
	managelinx common	device.dna. system.change. number		
		device.config. name		
		device.dna. system.change. timestamp		
	managelinx network interface	device.dna. system.network. iface.name		
		device.dna. system.network. iface.ipaddress		
	plaintext dsm credentials	dna.xml. replication. protocol.version		

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
ppp	authentication mode		pap	
			ms-chap	
			ms-chapv2	
			chap	
			none	
	local ip			Specifies both the address and mask.Use CIDR form (192.168.0.1/16) or explicit mask (192.168.0.1 255.255.0.0)
	password			If configured and not exporting secrets, exports only a placeholder.
	peer ip			
	username			
query port	state		disable	
			enable	
rss	feed		disable	
			enable	
	max entries			
	persist		disable	
			enable	
serial command mode	echo serial string		disable	
			enable	
	mode		disable	
			serial string	
			always	
	serial string			
	signon message			
	wait time			Milliseconds.
snmp	read community			If configured and not exporting secrets, exports only a placeholder.

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	state		enable	
			disable	
	system name			
	system contact			
	system description			
	system location			
	traps	state	disable	
			enable	
		primary destination		
		secondary destination		
	write community			If configured and not exporting secrets, exports only a placeholder.
ssh	max sessions			
	port			
	state		enable	
			disable	
ssh client	client user	private dsa key		If configured and not exporting secrets, exports only a placeholder.
		public dsa key		
		private rsa key		If configured and not exporting secrets, exports only a placeholder.
		public rsa key		
		password		If configured and not exporting secrets, exports only a placeholder.
		remote command		
	client user delete	name		Specify the user to delete.
	delete client users		disable	If enabled, deletes any existing client users before adding “client user”.
			enable	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	delete known hosts		disable	If enabled, deletes any existing hosts before adding “known host”.
			enable	
	known host	public rsa key		
		public dsa key		
	known host delete	name		Specify the known host to delete.
ssh server	authorized user	password		If configured and not exporting secrets, exports only a placeholder.
		public rsa key		
		public dsa key		
	authorized user delete	name		Delete an SSH authorized user.
	delete authorized users		enable	If enabled, deletes any authorized users before adding “authorized user”.
			disable	
	host dsa keys	public key		
		private key		If configured and not exporting secrets, exports only a placeholder.
	host rsa keys	public key		
		private key		If configured and not exporting secrets, exports only a placeholder.
ssl	delete all cas		disable	If enabled, deletes any existing trusted cas before adding “trusted ca”.
			enable	
	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.

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	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.
syslog	host			
	local port			
	remote port			
	severity log level		emergency	
			alert	
			critical	
			error	
			warning	
			notice	
			information	
			debug	
	state		disable	
			enable	
tcp	ack limit			Number of packets received before an ACK is forced.
	resets		disable	
			enable	
	send data		expedited	
			standard	
telnet	max sessions			
	port			
	state		enable	
			disable	
terminal	break duration			milliseconds
	echo		disable	
			enable	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	exit connect menu		disable	
			enable	
	login connect menu		disable	
			enable	
	send break			control character
	terminal type			
tftp server	allow file creation		disable	
			enable	
	allow firmware update		disable	
			enable	
	allow xcr import		enable	
			disable	
	state		disable	
			enable	
tunnel accept	accept mode		disable	
			any character	
			start character	
			modem control asserted	
			modem emulation	
			always	
	aes decrypt key			If configured and not exporting secrets, exports only a placeholder.
	aes encrypt key			If configured and not exporting secrets, exports only a placeholder.
	block network		disable	
			enable	
	block serial		disable	
			enable	
	cp output	group		

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
		connection value		
		disconnection value		
	email connect			
	email disconnect			
	flush serial		disable	
			enable	
	flush start character		enable	
			disable	
	local port			
	password	prompt	disable	
			enable	
		password		If configured and not exporting secrets, exports only a placeholder.
	protocol		tcp aes	
			ssh	
			ssl	
			telnet	
			tcp	
	start character			
	tcp keep alive			Milliseconds
tunnel connect	block serial		disable	
			enable	
	block network		disable	
			enable	
	connect mode		disable	
			any character	
			start character	
			modem control asserted	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
			modem emulation	
			always	
	cp output	group		cp group name
		connection value		
		disconnection value		
	email connect			
	email disconnect			
	flush serial		disable	
			enable	
	flush start character		enable	
			disable	
	host	vip	enable	
			disable	
		vip name		
		address		
		port		
		protocol	tcp	
			ssh	
			ssl	
			tcp aes	
			telnet	
			udp	
			udp aes	
		ssh username		
		tcp keep alive		
		aes encrypt key		
		aes decrypt key		
	host mode		Sequential	
			Simultaneous	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	local port			Either a specific number or “Random”.
	protocol		udp	
			ssh	
			ssl	
			tcp aes	
			udp aes	
			telnet	
	reconnect time			Milliseconds.
	start character			
tunnel disconnect	flush stop character		enable	
	flush serial		disable	
			enable	
	modem control		disable	
			enable	
	stop character		disable	
			enable	
	timeout			Milliseconds. A value of 0 disables the timeout.
tunnel modem	connect string		disable	
	display remote ip		disable	
			enable	
	echo commands		disable	
			enable	
	echo pluses		disable	
			enable	
	error unknown commands		disable	
			disabled	
	verbose response		disable	
			enable	
	response type		numeric	
			text	

Table 5-1 XCR Import and Export Groups (continued)

Group: Subgroup Name	Item Name	Value Name	Value	Description
	incoming connection		automatic	
			manual	
			disable	
tunnel packing	packing mode		timeout	
			send character	
			disable	
	send character			
	threshold			Bytes
	timeout			Milliseconds
	trailing character			
tunnel serial	buffer size			Bytes
	dtr		continuously asserted	
			unasserted	
			asserted while connected	
vip	state		enable	
			disable	
xml import control	cpm group delete	name		Deletes the specified cpm group.
	delete cpm groups		enable	Deletes existing groups before importing new ones.
			disable	
	delete http authentication uris		enable	Deletes existing http authentication uris before importing new ones.
			disable	
	http authentication uri delete	name		Deletes the specified http authentication uri.
	reboot		enable	Reboots after importing.
			disable	
	restore factory configuration		disable	
			enable	

XSR Groups and Items

Table 5-2 lists the supported XSR groups and items. The 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 in that the XSR allows groups within groups. The only XSR groups that contain sub-groups are buffer pools and tunnel. The buffer pools group has the following sub-groups:

- ethernet driver
- line
- protocol stack

The tunnel group contains the tunnel modem sub-group.

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values

Group: Subgroup Name	Item Name	Value Name	Valid Values
arp	arp entry	ip address	
		mac address	
		age	
		type	
buffer pool: ethernet driver	buffer headers	total	
		free	
		used	
		max used	
	cluster pool	cluster size	
		total	
		free	
		used	
		max used	
buffer pool: line	buffer headers	total	
		free	
		used	
		max used	
	cluster pool	cluster size	
		total	
		free	
		used	
		max used	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
buffer pool: protocol stack	buffer headers	total	
		free	
		used	
		max used	
	cluster pool	cluster size	
		total	
		free	
		used	
		max used	
cp group	cp	value	
		level	low
			high
		logic	inverted
			not inverted
		position	
	state		disabled
			disabled and locked
			enabled
			enabled and locked
			disabled and locked
	value		
cps	cp	pin	
		configured as	input
			output
		value	
		level	low
			high
		logic	inverted
			not inverted
		active group	
		group	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
device	product info	product type	
		serial number	
		firmware version	
		uptime	
		permanent config	saved
			unsaved
email	failed		
	queued		
	success	sent	
		sent with retries	
email log	entry	time	
		log	
filesystem	banks	current	
		firmware begin	
		firmware end	
		firmware erase cycles	
		firmware 2 begin	
		firmware 2 end	
		firmware 2 erase cycles	
		bank a begin	
		bank a end	
		bank a erase cycles	
		bank b begin	
		bank b end	
		bank b erase cycles	
	entries	file count	
		directory count	
		system count	
		open count	
		lock count	
		share count	
	filesystem	size	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
		available clean	
		available dirty	
		used total	
		used data	
		busy	
ftp	connections	rejected	
		accepted	
	last client	ip address	
		port	
	status		enabled
			disabled
hardware	cpu	type	
		speed	
	memory	flash size	
		ram size	
http	logging	state	enabled
			disabled
		max entries	
		format	
		entries	
		bytes	
	max bytes		
	max timeout		
	ports	http port	
		https port	
	state		enabled
			disabled
http log	entry		
	totals	entries	
		bytes	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
icmp	in	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	
	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	
		errors	
	ethernet (present only for eth0)	speed	
		duplex	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
interface	arp	encapsulation	
		type	
		timeout	
	default gateway		
	domain		
	generic	status	no link
			link up
			disabled
			unknown
		errors	
	hostname		
	ip address		
	last change		
	mac address		
	mtu		
	network mask		
	primary dns		
	receive	octets	
		unicast	
		non unicast	
		discards	
		errors	
		broadcast packets	
		multicast packets	
		filtered packets	
		unknown protocol	
		framing errors	
		overflows	
		crc errors	
		missed frame errors	
	secondary dns		
	transmit	octets	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
		unicast	
		non unicast	
		discards	
		errors	
		broadcast packets	
		multicast packets	
		filtered packets	
		deferred	
		multiple retries	
		one retry	
		underflows	
		late collisions	
		retry errors	
		carrier lost errors	
ip	default ttl		
	forwarded		
	fragments	needed	
		failures	
		success	
	in	receives	
		header errors	
		address errors	
		unknown protocols	
		discarded	
		delivered	
	out	requests	
		discards	
		discards no route	
	reassembly	timeout	
		needed	
		success	
		failures	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
	route discards		
	state		enabled
			disabled
ip sockets	ip socket	protocol	
		rx queue	
		tx queue	
		local address	
		local port	
		remote address	
		remote port	
		state	
line	line levels	cts	
		rts	
		dsr	
		dtr	
	receiver	bytes	
		breaks	
		parity errors	
		framing errors	
		overrun errors	
		no receive buffer errors	
		queued bytes	
		flow control	
	transmitter	bytes	
		breaks	
		queued bytes	
		flow control	
line: line	baud rate		Any value from 300 to 230400.
			odd
	data bits		7
			8

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
	flow control		hardware
			none
			software
	parity		even
			none
	protocol		lpd
			none
			ppp
			tunnel
	state		enable
			disable
	stop bits		1
			2
	xon char		enabled
			disabled
	xoff char		enabled
			disabled
lpd	bytes printed		
	current client ip address		
	current client port		
	last client ip address		
	last client port		
	jobs printed		
memory	main heap	condition	clean
		total memory	
		available memory	
		fragments	
		allocated blocks	
processes	process	pid	
		cpu %	
		stack used	

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
		stack size	
		thread name	
query port	last connection	ip address	
		port	
	in	discoveries	
		unknown queries	
		erroneous packets	
	out	discovery replies	
		errors	
	status		enabled
			disabled
rss	data	entries	
		bytes	
	url		
sessions	line	baud	
		parity	
		data bits	
		stop bits	
		flow control	
	ssh	local port	
		remote ip address	
		remote port	
		duration	
	telnet	local port	
		remote ip address	
		remote port	
		duration	
ssh	totals	uptime	
		bytes in	
		bytes out	
	state		

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
syslog	messages failed		
	messages send		
	status		
tcp	connections	maximum	
		open active	
		open passive	
		failed	
		resets	
		established	
	errors in		
	resets	in	
		out	
	segments	in	
		out	
		retransmitted	
	retransmission	algorithm	
		timeout minimum	
		timeout maximum	
telnet	state		enabled
			disabled
	totals	uptime	
		bytes in	
		bytes out	
tftp	downloaded		
	errors	read	
		write	
		unknown	
	last client	ip address	
		port	
	not found		
	status		enabled
			disabled

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
	uploaded		
tunnel	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: tunnel modem	echo commands		enable
			disable
	error unknown commands		enable
			disable
	incoming connection		enabled
			disabled
	response type		text
	verbose response		enable
			disable
udp	in datagrams		
	in errors		
	in unknown ports		
	out datagrams		
vip	conduit status		up
			down
	conduit uptime		
	config name		
	current tunnel port		
	dsm ip address		

Table 5-2 XSR Groups, Subgroups, Items, Value Names, and Valid Values (continued)

Group: Subgroup Name	Item Name	Value Name	Valid Values
	local dna id		
	time of last replication		
	tunnel port list		
	tunnel user		
xsr	errors		
	out	bytes	
		lines	
		elements	

MatchPort AR Commands and Levels

- root
  - enable (enable)
    - chem 1 (chem:1)
    - chem 2 (chem:2)
    - chem 3 (chem:3)
    - chem 4 (chem:4)
    - configure (config)
      - arp (config-arp)
      - cli (config-cli)
        - ssh (config-cli-ssh)
        - telnet (config-cli-telnet)
      - ftp (config-ftp)
      - host 1 (config-host:1)
      - host 2 (config-host:2)
      - http (config-http)
      - icmp (config-icmp)
      - if 1 (config-if:eth0)
        - link (config-ethernet:eth0)
      - ip (config-ip)
      - ip filter (config-filter)
      - lpd 1 (config-lpd:1)
      - lpd 2 (config-lpd:2)
      - query port (config-query_port)
      - rss (config-rss)
      - snmp (config-snmp)
      - 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)
    - cpm (cpm)
    - device (device)
    - filesystem (filesystem)
    - line 1 (line:1)
    - line 2 (line:2)
    - lpd (lpd)
    - ppp 1 (ppp:1)
    - ppp 2 (ppp:2)
    - ssh (ssh)
    - ssl (ssl)
    - tunnel 1 (tunnel:1)
      - accept (tunnel-accept:1)
        - cp output (tunnel-

▪ host 2 (tunnel-connect-host:2:2) ▪ host 3 (tunnel-connect-host:2:3) ▪ host 4 (tunnel-connect-host:2:4) ▪ host 5 (tunnel-connect-host:2:5) ▪ host 6 (tunnel-connect-host:2:6) ▪ host 7 (tunnel-connect-host:2:7) ▪ host 8 (tunnel-connect-host:2:8) ▪ host 9 (tunnel-connect-host:2:9) ▪ host 10 (tunnel-connect-host:2:10) ▪ host 11 (tunnel-connect-host:2:11) ▪ host 12 (tunnel-connect-host:2:12) ▪ host 13 (tunnel-connect-host:2:13) ▪ host 14 (tunnel-connect-host:2:14) ▪ host 15 (tunnel-connect-host:2:15) ▪ host 16 (tunnel-connect-host:2:16) ▪ disconnect (tunnel-disconnect:2) ▪ modem (tunnel-modem:2) ▪ packing (tunnel-packing:2) ▪ serial (tunnel-serial:2)	
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.
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 <*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.
chem 1 (chem:1) level commands	
auto show statistics	Continuously displays email statistics.
cc <*email addresses*>	Sets Cc addresses for email alerts. <email addresses> = a semicolon-separated list of email addresses within quotation marks (For example, “name1; name2”)

chem <*number*>	Enters the configure email level.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
exit	Exits to the enable level.
file <*file*>	Specifies a text file, the contents of which will be the message body of an email alert. <file> = the name of a local file.
from <*email address*>	Sets the From address for email alerts. <email address> = email address to list in the From field of the email alert.
local port <*number*>	Sets local port used to send email alerts. <number> local port to use for email alerts.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no file	Removes the file name, so the message body will be empty.
no from	Removes From address for email alerts.
no overriding domain	Removes the overriding domain name option.
no replyto	Removes Reply-To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes To address for email alerts.
no trigger	Disables the trigger to send an email.
overriding domain <*domain*>	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. <domain> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2.
priority low	Sets X-Priority for email alerts to 4.
priority normal	Sets X-Priority for email alerts to 3.
priority urgent	Sets X-Priority for email alerts to 1.
priority very low	Sets X-Priority for email alerts to 5.
replyto <*email address*>	Sets Reply-To address for email alerts. <email address> = email address to list 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 email settings.
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 <*string*>	Sets the subject for email alerts. <string> = text to placed as the subject.
to <*email addresses*>	Sets email address to which the email alerts will be sent. <email addresses> = a quoted, semi-colon separated list of email addresses.
trigger <*cp group*> <*value*>	Specify a CP group and its value that shall trigger an email. <cp group> = configurable pin group. <value> = 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.
chem 2 (chem:2) level commands	
auto show statistics	Continuously displays email statistics.
cc <*email addresses*>	Sets Cc addresses for email alerts. <email addresses> = a semicolon-separated list of email addresses within quotation marks (For example, “name1; name2”)
chem <*number*>	Enters the configure email level.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
exit	Exits to the enable level.
file <*file*>	Specifies a text file, the contents of which will be the message body of an email alert. <file> = the name of a local file.
from <*email address*>	Sets the From address for email alerts. <email address> = email address to list in the From field of the email alert.
local port <*number*>	Sets local port used to send email alerts. <number> local port to use for email alerts.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no file	Removes the file name, so the message body will be empty.
no from	Removes From address for email alerts.

no overriding domain	Removes the overriding domain name option.
no replyto	Removes Reply-To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes To address for email alerts.
no trigger	Disables the trigger to send an email.
overriding domain <*domain*>	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. <domain> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2.
priority low	Sets X-Priority for email alerts to 4.
priority normal	Sets X-Priority for email alerts to 3.
priority urgent	Sets X-Priority for email alerts to 1.
priority very low	Sets X-Priority for email alerts to 5.
replyto <*email address*>	Sets Reply-To address for email alerts. <email address> = email address to list 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 email settings.
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 <*string*>	Sets the subject for email alerts. <string> = text to placed as the subject.
to <*email addresses*>	Sets email address to which the email alerts will be sent. <email addresses> = a quoted, semi-colon separated list of email addresses.
trigger <*cp group*> <*value*>	Specify a CP group and its value that shall trigger an email. <cp group> = configurable pin group. <value> = 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.
chem 3 (chem:3) level commands	
auto show statistics	Continuously displays email statistics.

cc <*email addresses*>	Sets Cc addresses for email alerts. <email addresses> = a semicolon-separated list of email addresses within quotation marks (For example, “name1; name2”)
chem <*number*>	Enters the configure email level.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
exit	Exits to the enable level.
file <*file*>	Specifies a text file, the contents of which will be the message body of an email alert. <file> = the name of a local file.
from <*email address*>	Sets the From address for email alerts. <email address> = email address to list in the From field of the email alert.
local port <*number*>	Sets local port used to send email alerts. <number> local port to use for email alerts.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no file	Removes the file name, so the message body will be empty.
no from	Removes From address for email alerts.
no overriding domain	Removes the overriding domain name option.
no replyto	Removes Reply-To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes To address for email alerts.
no trigger	Disables the trigger to send an email.
overriding domain <*domain*>	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. <domain> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2.
priority low	Sets X-Priority for email alerts to 4.
priority normal	Sets X-Priority for email alerts to 3.
priority urgent	Sets X-Priority for email alerts to 1.
priority very low	Sets X-Priority for email alerts to 5.
replyto <*email address*>	Sets Reply-To address for email alerts. <email address> = email address to list 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 email settings.
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 <*string*>	Sets the subject for email alerts. <string> = text to placed as the subject.
to <*email addresses*>	Sets email address to which the email alerts will be sent. <email addresses> = a quoted, semi-colon separated list of email addresses.
trigger <*cp group*> <*value*>	Specify a CP group and its value that shall trigger an email. <cp group> = configurable pin group. <value> = 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.
chem 4 (chem:4) level commands	
auto show statistics	Continuously displays email statistics.
cc <*email addresses*>	Sets Cc addresses for email alerts. <email addresses> = a semicolon-separated list of email addresses within quotation marks (For example, “name1; name2”)
chem <*number*>	Enters the configure email level.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
exit	Exits to the enable level.
file <*file*>	Specifies a text file, the contents of which will be the message body of an email alert. <file> = the name of a local file.
from <*email address*>	Sets the From address for email alerts. <email address> = email address to list in the From field of the email alert.
local port <*number*>	Sets local port used to send email alerts. <number> local port to use for email alerts.
no cc	Removes the Cc addresses for email alerts.

no clear mail counters	Restores the email counters to the aggregate values.
no file	Removes the file name, so the message body will be empty.
no from	Removes From address for email alerts.
no overriding domain	Removes the overriding domain name option.
no replyto	Removes Reply-To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes To address for email alerts.
no trigger	Disables the trigger to send an email.
overriding domain <*domain*>	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. <domain> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2.
priority low	Sets X-Priority for email alerts to 4.
priority normal	Sets X-Priority for email alerts to 3.
priority urgent	Sets X-Priority for email alerts to 1.
priority very low	Sets X-Priority for email alerts to 5.
replyto <*email address*>	Sets Reply-To address for email alerts. <email address> = email address to list 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 email settings.
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 <*string*>	Sets the subject for email alerts. <string> = text to placed as the subject.
to <*email addresses*>	Sets email address to which the email alerts will be sent. <email addresses> = a quoted, semi-colon separated list of email addresses.
trigger <*cp group*> <*value*>	Specify a CP group and its value that shall trigger an email. <cp group> = configurable pin group. <value> = 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.
cli (config-cli)	
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.
configure (config) level commands	
arp	Changes to the command level for ARP configuration and status.
clear host <*host*>	Removes an entry from the DNS Cache
cli	Change to menu level for CLI configuration and status
clrscrn	Clears the screen.
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.
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.
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
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 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 disconnection.
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 disconnection.
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_ar	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.
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.
enable (enable) level commands	
auto show interfaces	Show interface statistics
auto show processes	Continuously show thread runtime information
auto show xsr	Show XML Status Record counters
chem <*number*>	Enters the configure email level.
clear interfaces counters	Zeros interface session counters
clear query port counters	Zeros Query Port counters

clear xsr counters	Zeros XML Status Record 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.
exit	Exit from the system
filesystem	Enters the filesystem level.
kill line <*line*>	Kills command mode session on the Line
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
no clear query port counters	Unzeros Query Port counters
no clear xsr counters	Unzeros XML Status Record counters
nslookup	Lookup host information for the given host name
nslookup <*host*>	Return host information for the given host name
ping <*host*>	Ping destination 5 times 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
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	Show system information
show history	Displays the last 20 commands entered during the current CLI session.

show hosts	Show domain settings
show interfaces	Show interface statistics
show ip sockets	Show UDP/TCP state information
show matchport_ar	Show system information
show processes	Show thread runtime information
show sessions	Show active Telnet and SSH Sessions
show xsr	Show XML Status Record counters
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.
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

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.
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.
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.
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.
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: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.
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.
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: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.
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.
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: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.
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.
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: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 punctuation: 123ABC "12 3A BC" 12,3A,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.
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.
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: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.
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.
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: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.
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.
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: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.
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.
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.
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.
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: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.
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.
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: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.
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.

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: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.
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.

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: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.
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.
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: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.
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.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:2:9) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
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.
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.
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.
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.
clear counters	Sets the HTTP counters to zero.
clear log	Clears the HTTP server log.
clrscrn	Clears the screen.
default log format	Restores the HTTP Server log format string to its default

	value.
default log max entries	Restores the default maximum number of HTTP Server log entries.
default max bytes	Resets the default maximum bytes the HTTP Server will accept when receiving a request.
default max timeout	Resets the default maximum time the HTTP Server will wait when receiving a request.
default port	Resets the HTTP Server port to its default value.
default ssl port	Resets the HTTP Server SSL port to its default value.
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 disable	Disables HTTP server logging.
log enable	Enables HTTP server logging.
log format <*string*>	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
max bytes <*bytes*>	Sets the maximum number of bytes the HTTP server accepts when receiving a request.
max timeout <*seconds*>	Sets the maximum timeout the HTTP server waits when receiving a request. <seconds> = maximum timeout value.
no clear counters	Restores the HTTP counters to the aggregate values.
port <*number*>	Sets the port number the HTTP server will use.

	<number> = port number.
server disable	Disables the HTTP server.
server enable	Enables the HTTP server.
show	Displays the HTTP server settings.
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.
ssl port <*number*>	Sets the port number the HTTP server will use over SSL. <number> = port number.
ssl3 disable	Disables SSLv3 handling.
ssl3 enable	Enables SSLv3 handling.
tls1.0 disable	Disables TLSv1.0 handling.
tls1.0 enable	Enables TLSv1.0 handling.
tls1.1 disable	Disables TLSv1.1 handling.
tls1.1 enable	Enables TLSv1.1 handling.
write	Stores the current configuration in permanent memory.
icmp (config-icmp) level commands	
auto show stats	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 stats	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.
clear host <*string*>	Removes an entry from the DNS Cache
clrscrn	Clears the screen.

default gateway *<ip address>*	Sets the configurable gateway IP address to the default value.
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.
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
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
write	Stores the current configuration in permanent memory.
ip (config-ip) level commands	
auto show stats	Continuously shows IP statistics
clear counters	Zeros counters
clrscrn	Clears the screen.
default multicast time to live	Restores the default IP multicast time to live, which is one hop.

exit	Exits to the configuration level.
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 stats	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.
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.
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> = any rate between 300 and 230400.
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.
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.
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 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> = any rate between 300 and 230400.
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.
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.
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 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-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.
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 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.
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	
clrscrn	Clears the screen.
exit	Returns to the config level.

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 5 times 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_ar	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.
serial (tunnel-serial:2) level commands	
buffer size <*bytes*>	Sets the size of the buffer for data read from the serial port. <bytes> = size of the buffer.

clrscrn	Clears the screen.
default buffer size	Restores the default buffer size.
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	
buffer size <*bytes*>	Sets the size of the buffer for data read from the serial port. <bytes> = size of the buffer.
clrscrn	Clears the screen.
default buffer size	Restores the default buffer size.
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.
snmp (config-snmp) level commands	
clrscrn	Clears the screen.
community ro <*string*>	Sets the SNMP read-only community string. <string> = name of the read-only community string to be set.
community rw <*string*>	Sets the SNMP read-write community string. <string> = name of the read-write community string to be set.

contact <*string*>	Sets the SNMP system contact information. <string> = system contact information.
default description	Restores the SNMP system description to its default.
description <*string*>	Sets the SNMP system description. <string> = description of device.
exit	Returns to the config level.
host <*ip address*>	Sets the primary SNMP trap host. <IP address> = IP address of host running the SNMP trap.
host <*ip address*> <*ip address*>	Sets the primary and secondary SNMP trap hosts. <IP address> = IP address of primary host running the SNMP trap. <IP address> = IP address of secondary host running the SNMP trap.
location <*string*>	Sets the SNMP system location. <string> = location of device.
name <*string*>	Sets the SNMP system name. <string> = SNMP system name.
no community ro	Clears the SNMP read-only community.
no community rw	Clears the SNMP read/write community.
no contact	Clears the SNMP server contact.
no host <*ip address*>	Deletes the designated SNMP server trap host. <IP address> = IP address of an SNMP server.
no location	Clears the SNMP server location.
no name	Clears the SNMP server name.
server disable	Disables the SNMP server.
server enable	Enables the SNMP server.
show	Displays the SNMP server settings.
show history	Displays the last 20 commands entered during the current CLI session.
traps disable	Disables the sending of SNMP trap messages.
traps enable	Enables the sending of SNMP trap messages.
write	Stores the current configuration in permanent memory.
ssh (ssh) level commands	
client server <*server*>	Set Client Server RSA or DSA key
client server <*server*> <*key*>	Set Client Server RSA or DSA key
client user <*user*> <*command*>	Set Client User, command and RSA or DSA keys
client user <*user*> <*password*> <*command*>	Set Client User with password, command and optional RSA or DSA keys
client user <*user*> <*password*> <*command*>	Set Client User with password, command and RSA or DSA

<*public*> <*private*>	keys
client user <*user*> generate dsa 1024	Generate DSA public and private keys
client user <*user*> generate dsa 512	Generate DSA public and private keys
client user <*user*> generate dsa 768	Generate DSA public and private keys
client user <*user*> generate rsa 1024	Generate RSA public and private keys
client user <*user*> generate rsa 512	Generate RSA public and private keys
client user <*user*> generate rsa 768	Generate RSA public and private keys
clrscrn	Clears the screen.
exit	Exits to the enable level.
host	Sets RSA or DSA public and/or private keys
host <*key*>	Sets RSA or DSA public or private key
host <*public*> <*private*>	Sets RSA or DSA public and private keys
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 user <*user*> <*password*>	Sets Host username and password
host user <*user*> <*password*> <*public*>	Sets Host username, password and either a RSA or DSA public key. Place the entire contents of the file generated by ssh-keygen within quotes.
host user <*user*> <*password*> <*public*> <*public*>	Sets Host username, password and both RSA and DSA public keys. For each key, place the entire contents of the file generated by ssh-keygen within quotes.
no client server <*server*>	Remove Client Server
no client server <*server*> dsa	Remove Client Server DSA key
no client server <*server*> rsa	Remove Client Server RSA key
no client user <*user*>	Remove Client User
no client user <*user*> command	Remove command from Client User
no client user <*user*> dsa	Remove Client User DSA key
no client user <*user*> rsa	Remove Client User RSA key
no host dsa	Removes DSA public and private keys
no host rsa	Removes RSA public and private keys

no host user <*user*>	Remove a host user
show	Show SSH settings
show client server <*server*>	Show Client Server RSA and DSA keys
show client user <*user*>	Show information for a client 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
show host user <*user*>	Show information for a host user
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 stats	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 send data	Sets TCP to send data in accordance with standards.
exit	Exits to the configuration level.
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 sufficiently 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 stats	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 configured.
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.
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 stats	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 stats	Shows UDP statistics

write	Stores the current configuration in permanent memory.
vip (config-vip) level commands	
auto show statistics	Displays VIP statistics 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 history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the VIP statistics.
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.