USER'S GUIDE
Vertical Console Port Server

Contents

Introduction

Product Description

Features

The American Power Conversion (APC®) Vertical Console Port Server (VCPS) allows both local and remote access for in-band and out-of-band network management. It is a zero-U, rack-mountable server that can be used to monitor and manage up to 42 servers or other devices with serial consoles within a rack.

The VCPS has the following features:

- 42 serial ports
- One Ethernet port with two status LEDs
- One configuration serial port
- A recessed **Reset** button

The VCPS can be mounted vertically to the rear of a NetShelter® VX Enclosure or with mounting brackets in any standard enclosure.

You can access the VCPS using any of these methods:

- A console directly connected to a VCPS
- Telnet/SSH over a network
- SNMP for MIB II OIDs and traps

All configuration, monitoring, and management is done through the Command Line Interface (CLI).

Parameter/command syntax and terminology conventions. This manual uses the following syntax and conventions for parameters, commands, and terms:

- Brackets and hyphens:

  Brackets ([ ]) indicate that the enclosed parameter is optional. The command will be accepted if the parameter is not defined. When the text enclosed by the brackets starts with a hyphen (-) or indicates a list of characters, the parameter can be one of the letters within the brackets.

  Example:

  `dhcp set [-v <vendor-class>] [-c <client-ID>] [-u <user-class]`

- Pipes:

  A pipe (|) between words indicates that one of the words must be used in the command.

  Example:

  `snmp [enable|disable]`

- Greater-than and less-than signs:

  Text enclosed by the <> characters and in italic font is variable, not literal text. You must replace the enclosed italic text with a literal value.

  Example:

  `cps disconnect <user>`

- Italic text:

  Italic text is used for the following.

  – File and directory names

  – New terms being defined

  – Variable text, which is also enclosed by the characters < >.

Installation and Configuration

Set-up and Configuration

Initial set-up

If you are not using DHCP (enabled by default) you must define three TCP/IP settings for the VCPS before it can operate on the network:

- IP address of the VCPS
- Subnet mask
- IP address of the default gateway

To use a DHCP server to configure the TCP/IP settings for a VCPS, see DHCP and BOOTP configuration.

How to log on

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection to access the control console.

Use case-sensitive user name (login) and password entries to log on (by default, **apc** and **apc** for the Permanent Administrator).

If you cannot remember your login or password, see How to recover from a lost password.

Remote access to the control console

You can access the CLI through Telnet or SSH, depending on which is enabled. (An administrator can enable these access methods through the CLI.) Both Telnet and SSH are enabled by default.

See Telnet and SSH for details on how to use these protocols to access the control console.

Local access to the control console

You can use a local computer to access the control console.

1. Select a serial port such as COM1 or COM2 at the local computer and disable any service which uses that port.
2. Connect the cable (APC part number 940-0214) to the selected port at the local computer and to the configuration port of the VCPS.
3. Run a terminal program (such as HyperTerminal®), and configure the selected port as follows:
   - 9600 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control

   Save the changes.
4. Press ENTER to display the **login** prompt.
5. Enter your user name and password.

How to recover from a lost password

Any administrator can change any password, including the password for the permanent administrator. If all administrator passwords are lost, the entire configuration of the unit must be reset to defaults.

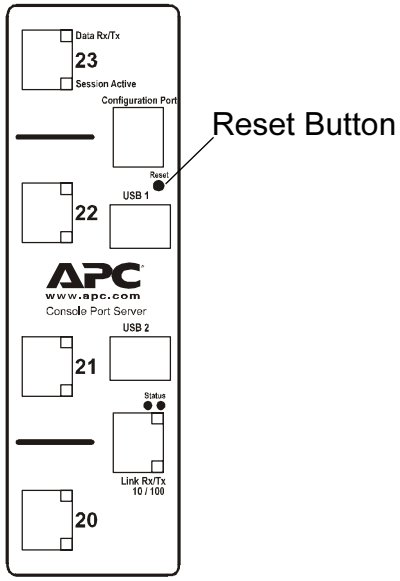
Pressing the **Reset** button for ten seconds resets **all** VCPS settings.

You can reset the user name and password for VCPS.

1. Press and hold the **Reset** button on the VCPS for 10 seconds. The status LED will turn from solid green to solid orange.
2. After 10 seconds, the orange LED will blink four times. Release the button.
3. The status LED will be solid orange and then begin blinking as VCPS restores its defaults. This will take up to 2 minutes.
4. The status LED will blink green when defaults have been restored.

The permanent administrator user name and password will be reset to the default of **apc**. All other users will be deleted. For proper security, change the password immediately.

The following illustration shows the location of the **Reset** button on the VCPS front panel.



TCP/IP configuration

You can manually configure your TCP/IP settings using the **`network`** command in the CLI. Enter:

```
network set -b static
```

Note

See network for details on how to configure your TCP/IP settings manually.

To set your TCP/IP settings automatically, enter:

```
network set -b dhcp
```

Note

See DHCP and BOOTP configuration for details on how to configure your TCP/IP settings using DHCP or BOOTP.

DHCP and BOOTP configuration

In addition to using manual (static) settings, the VCPS can use a Dynamic Host Configuration Protocol (DHCP) server to provide the settings the VCPS needs to operate on a TCP/IP network. The VCPS can also obtain TCP/IP settings from BOOTP while operating in DHCP mode.

DHCP is enabled by default. To disable or enable DHCP, use the **`network set mode`** command in the CLI. Use the **`dhcp`** command in the CLI to set DHCP options.

For details on how to configure DHCP using the CLI, see dhcp.

For information on DHCP and DHCP options, see RFC2131 and RFC2132 at **www.ietf.org/rfc.html**.

The VCPS makes requests for its network assignment from any DHCP or BOOTP server. If a valid DHCP or BOOTP response is received, the VCPS starts the network services. If the VCPS does not receive a valid DHCP or BOOTP response, it waits 10 seconds and makes the request again. If there is still no response after the timeout interval of 60 seconds, it waits 5 minutes and starts the cycle over. It continues sending BOOTP and DHCP requests until it receives a valid network assignment.

For more information on what a valid response requires, see DHCP response options.

DHCP Configuration Settings

DHCP request options

Use the **dhcp** command in the command line interface to configure the **Vendor Class**, **User Class**, and **Client ID** settings of the VCPS.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings a VCPS needs to operate on a network and other information that affects the operation of the VCPS.

TCP/IP options. A VCPS uses the following options within a valid DHCP response to define its TCP/IP settings:

- **IP Address** (from the **yiaddr** field of the DHCP response): The IP address that the DHCP server is leasing to the VCPS.
- **Subnet Mask** (option 1): The subnet mask value which the VCPS needs to operate on the network.
- **Default Gateway** (option 3): The default gateway address, which the VCPS needs to operate on the network.
- **Address Lease Time** (option 51): The time duration for the lease associated with the identified IP Address.
- **Renewal Time, T1** (option 58): The time that the VCPS must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the VCPS must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. A VCPS uses the following options within a valid DHCP response to define Network Time Protocol (NTP), Domain Name System (DNS), hostname and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): VCPS accepts an NTP server list from which it extracts the first two servers.
- **DNS Server, Primary and Secondary** (option 6): Up to two DNS servers that can be used by the VCPS.
- **Host Name** (option 12): The host name to be used by the VCPS (32-character maximum length).
- **Domain Name** (option 15): The domain name to be used by the VCPS (64-character maximum length).

User Management

Overview

The system has a single default user, the permanent administrator. The default user name and password for the permanent administrator are **apc** and **apc**, both of which should be changed immediately for security purposes.

The permanent administrator can never be deleted from the system. This administrator can create and assign privileges to other administrators and users. There are four levels of access, each providing a different set of permissions. A user can be assigned only one access level.

Valid user names are 3 to 32 characters, can include both letters and numbers, are case-sensitive, cannot contain a space, and cannot start with a number. Valid passwords are 3 to 32 characters, can include letters, numbers, and symbols including spaces, are case-sensitive, and can start with a number.

These access levels are for local users and are configured and stored locally on the VCPS. For information on remote authentication, see RADIUS.

Administrator Access

A user with administrator access can configure all VCPS network and system parameters and connect to all VCPS ports.

Port-Admin Access

A port-admin user can configure all VCPS port parameters and access all ports. The port-admin user has access to the following port-specific commands. Some subcommands are restricted:

- clear
- cfg
- cps
- exit
- help
- ?
- ls
- port
- prompt
- quit
- version
- view

Port-Readonly Access

A port-readonly user can view some port parameters but does not have write access. The port-readonly user can connect to ports only in monitor mode. A port-readonly user has access to the following commands. Some subcommands are restricted:

- cps
- exit
- help
- ?
- ls
- port
- prompt
- quit
- version

Port Users

Port users can monitor port activity, or they can monitor and access assigned ports.

A port user can monitor or access multiple ports. Ports can be assigned as a port number, port name, or a range of ports. A port user can be assigned to have access to some ports and to only monitor others. For example:

```
user set bob -a 1,5-7:m;10,12:ma
```

This user can monitor ports 1, 5, 6 and 7, and can access ports 10 and 12.

Accessing the Serial Ports

Overview

You can access the VCPS serial console ports for attached servers or devices in the following ways:

- Local access to the CLI through the configuration port
- Telnet/SSH access to the CLI
- Telnet/SSH access directly to a specific console port

Telnet and SSH

You can access the console ports through the CLI using Telnet or SSH, using the **cps connect** *<port>* command. (An Administrator can enable Telnet or SSH through the CLI.)

You can also access a specific console port directly through Telnet or SSH using base port.

See Using Base Port for more information.

Telnet and SSH are both enabled by default.

See telnetd and sshd for more information on how to configure your VCPS for use with Telnet and SSH.

Telnet for basic access

Telnet provides the basic security of authentication by logon and password, but not the high-security benefits of encryption. To use Telnet to access the control console from any computer on the same network:

1. At a command prompt, type **telnet** and the System IP address for the VCPS (when the VCPS uses the default Telnet port of 23), and press ENTER. For example:

   ```
   telnet 139.225.6.133
   ```

   If the VCPS uses a non-default port number (between 5000 and 65535), include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter your user name (login) and password (by default, **apc** and **apc** for the permanent administrator).

SSH for high-security access

For high security, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

To use SSH to access the control console from any computer on the same network:

1. At a command prompt, type **ssh**, the username, the "at" (@) character, and the System IP address for the VCPS (when the VCPS uses the default SSH port of 22), and press ENTER. For example:

   ```
   ssh apc@139.225.6.133
   ```

   Note If the VCPS uses a non-default port number (between 5000 and 65535), include a colon or a space (depending on your SSH client) between the IP address and the port number.

2. Enter your user name (login) and password (by default, **apc** and **apc** for the permanent administrator).

Attaching Devices to Serial Ports

From the CLI, use the **cps connect** command and specify the port number or port name to attach a device to a serial port. For example, to connect a device to port 5, type:

```
cps connect 5
```

or

```
cps connect port5
```

A user with read-only access or monitor permission only can not write to a port. Any characters typed by that user at the keyboard are not sent to the device attached to the serial port. To attach in **spy** or read-only mode, type:

```
cps spy 5
```

or

```
cps spy port5
```

After you connect to a port, one of the following is displayed:

`Enter '^Ec?' for help` (if you have write access to the port)

`[read-only -- use '^Ec?' for help]` (if you have only monitor access to the port)

If two users access the same port, the first user to attach to the port has write access. The second user to attach to the port has read-only access, and the console displays the following message:

```
[no apc@157.204.7.10 is attached]
[read-only -- use '^Ec?' for help]
```

After the first user disconnects from the port, the second user has write access, and the console displays the following message:

```
[attached]
```

Type **^Ec** (CTRL +E, then c) to enter a command. In command mode, you can cause the VCPS to perform a number of actions such as disconnecting from a serial port, sending a break sequence, and sending a broadcast message to all users attached to serial ports. These commands are not directly relayed to the device attached to the serial port. (Some commands such as **send break** cause the VCPS to send characters to the attached device.) Following are some commonly used commands.

- To disconnect from a serial port, type `^Ec.` (CTRL +E, then c, followed by period)
- To send a hardware break, type `^Ecl0` (CTRL +E, then c, then lowercase L [l], then zero)
- To display a list of commands type `^Ec?` (CTRL +E, then c, then ?). After connecting to a port, you will see:

  ```
  Enter '^Ec?' for help
  ```

  The **^Ec** part is the escape sequence and **?** is the port command help.

Port Mode Commands and Escape Sequence

Special port mode commands are accessible using the escape sequence after you have attached to a serial port. The **disconnect** command detaches from the serial port and returns to the CLI or closes a direct Telnet or SSH session.

Using port mode commands

All port mode commands are preceded by the escape sequence. The default is **^Ec** (CTRL +E, then c) followed by one of the port mode commands from the table below. The **?** command displays all available commands, which are listed in the table.

Command Character	Description
.	Disconnect from a port
a	Attach read/write to a serial port
b	Send a broadcast message
c	Toggle flow control
e	Change the escape sequence
f	Force attach read/write
L	Toggle port logging on/off
l?	List the break sequences
l0	Send the default break sequence set for the port
l1-9	Send a specific break sequence
m	Display the message of the day
p	Replay the last 60 lines

Command Character	Description
r	Replay the last 20 lines
s	Attach to a port in spy mode (read-only)
w	Display who is attached to the port
?	Print command help
ENTER or <CR>	Ignore/abort command
^R (CTRL+R)	Replay the last line
\ooo	Send character by octal code

Escape sequence

The escape sequence is composed of the escape-character and the command mode character. Both of these characters can be redefined by an administrator using the **`cps set escapechar`** and **`cps set cmdmodechar`** commands.

For more information on the defining the escape and command mode characters, see the cps command.

Command macros

There are six single-character command macros that can be mapped to any of the port mode commands. The command macros are preceded by the escape-character to provide two-character shortcuts.

Examples

Set your command macros:

- **`cmd set macro1 A .`** - set the macro **`A`** to the disconnect command "**`.`**"
- **`cmd set macro2 B l0`** - set the macro **`B`** to send the default break sequence for port "**10**"

After you set your command macros and have attached to a port:

- Enter **`EA`** to disconnect
- Enter **`EB`** to send the default break sequence

Using Base Port

You can use Telnet/SSH to directly access a VCPS serial port using the base TCP port.

The base TCP port default is 9000. You can change the base port setting using the **`cps set`** command in the CLI to any unused TCP port from 5000 to 65493.

If you use Telnet to directly access a serial port, the following command would connect you directly to the server or device connected to port 5 on the VCPS at the IP address 157.204.7.12.

```
telnet 157.204.7.12 9005
```

When you use the base port to directly access a server or device, first enter your user name (login) and password for the CLI and then your user name (login) and password specific to the device.

If you use SSH to directly access a serial port, the following command would connect you directly to the server or device connected to port 5 on the VCPS at the IP address 157.204.7.12.

```
ssh -p 9005 apc@157.204.7.12
```

If the VCPS uses a non-default port number (between 5000 and 65493), include a colon or a space (depending on your SSH client) between the IP address and the port number.

See your SSH Client documentation for information on how to connect to a remote SSH server using a specific TCP port.

Using Direct Port Name Access With SSH

You can use SSH to directly access a VCPS serial port using **`username:portname`** syntax. In this example, a user named **`apc`** has access to a port on VCPS named **`webserv1`**.:

```
ssh apc:webserv1@157.204.7.12
```

Serial Port Logs

Overview

The Vertical Console Port Server logs all data received from an attached device to a file. There is one log file and one rolled log file for each port. Log files are stored in the `conlogs` directory on the VCPS, and are named <*port-name*>.

After the size of a port log file exceeds 100 Kilobytes, it rolls over to a rolled log file named <*port-name*>.0, and restarts logging with an empty log file. These files are accessible by an administrator using FTP or SCP.

Console port logging is disabled by default. See the CLI port command to enable logging for specific ports.

How to Use FTP or SCP to Retrieve Log Files

If you are an Administrator, you can use FTP or SCP to retrieve a port log file (<*port-name*>). The file reports all of the port traffic since the log was last deleted.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See Security for information on the available protocols and methods for setting up the type of security appropriate for your needs.

To use SCP to retrieve the files

To use SCP to retrieve the *eventlog* file, use the following command:

```
scp username@hostname_or_ip_address:/logs/messages ./
messages
```

To use SCP to retrieve the port log file, use the following command:

```
scp username@hostname_or_ip_address:/conlogs/<port-name> ./<port-name>
```

To use FTP to retrieve the files

To use FTP to retrieve the *eventlog* or <*port-name*> file:

1. At a command prompt, type `ftp` and the VCPS's IP address, and press ENTER.

   If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command,

including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

`ftp>open <ip-address> <port-number>`

To use non-default port values to enhance security, see Port assignments.

2. Use the case-sensitive **User Name** and **Password** for an Administrator to log on. For a permanent administrator, **apc** is the default for **User Name** and **Password**.
3. Change to the console logs directory:
   `cd conlogs`
4. Use the **get** command to transmit the port log to your local drive.
   `ftp>get <port-name>`
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Viewing the Log Using the CLI

You can use the CLI to display the log for a specific port.

For details on how to use the view command in the CLI to access the event and port logs, see view.

Using the Command Line Interface

Overview

The VCPS Command Line Interface (CLI) has the following features:

- command line editing
- history retrieval
- extensive help system

Command Line Interface

Structure and syntax

The CLI is composed of a set of commands that follow a basic syntax:

```
<command> <subcommand>[<target>][<option>
<argument>]...[<option> <argument>]
```


Note

The use of brackets [ ] in this guide indicates that the parameter is optional.

After you log in to the CLI, enter `help` to display a list of the commands that you have permission to use. A command is a specific order to the system to perform an action. A subcommand applies an operation to a command.

Each option must be followed by an argument.

```
[<option> <argument>]
```

You can use multiple `[<option> <argument>]`elements in one command.

Each option can be specified in short form (efficient) or in long form. The short form is specified with a single hyphen followed by a single letter:

```
-n
```

The long form is specified with a double hyphen followed by a keyword:

```
--name
```


Note

You must use a space to separate an option and its argument when using the long form. The space is optional when using the short form.

An argument is a character or string of characters.

Activating and saving VCPS configurations

When you finish executing a set subcommand, it is only set in the database. To activate your changes, you must execute the **`cfg run`** command to restart all services except the network (TCP\IP settings and DHCP). Use the **`cfg run - n`** command to restart all services and the network. The **`network restart`** command will restart only the network.

To save your changes to flash memory so they will be in effect when you reboot the system, you must execute the **`cfg save`** command.

Error messages

An error message is displayed when syntax rules are violated, the target range is incorrect, or the validation criteria are not met. The format of an error message depends on the level of the offending command line elements. Examples include:

- invalid argument
- command parameter error

Usage commands

Context-sensitive usage commands are displayed when you enter a question mark (**?**) on the command line.

Help statements

Enter one of the following statements on the command line to display help:

- **?** - Displays a list of all commands
- **help** - Displays a list of all commands with explanations
- **help <*command*>** - Displays help specific to the command you entered

History buffer

Press the up arrow key to display the last command line entered during your user session. Continue to press the up arrow key to display earlier command lines.

Press the down arrow key to display the first command line entered during your user session. Continue to press the down arrow key to move forward through the command line display.

User-level (authorization)

The permanent administrator is in charge of the system and can create other users and assign privileges. The permanent administrator can create multiple administrative users.The permanent administrator can never be deleted as an administrative user.

For details on users and permissions, see User Management.

VCPS CLI Commands

Click on a command to view usage details.

Command	Use This Command To
cfg	Save or load the VCPS system configuration to a non-volatile database.
clear	Clear the event or console logs.
cps	Configure and administer console port service.
date	Set the system date, time, and time zone; show the current system date, time and time zone.
dhcp	Set or display the DHCP configuration, or restart the DHCP interface.
exit	End a session and log out.
ftpd	Configure or display the FTP configuration.
help	Display a list of commands or, using help <*command*>, display command-specific help.
?	Display context-sensitive help.
loadfw	Load firmware to the VCPS.
ls	List files in the current working directory.
network	Set or display the network configuration, show the network status, or restart the network interface.
ntp	Set or display the NTP configuration, or restart the NTP interface.
ping	Verify that the device at an IP address that you enter exists and can accept requests.
port	Set or display a port's configuration, or restart a port server.
prompt	Set the command prompt form.
radius	Set or display a RADIUS server configuration, or restart a RADIUS client.
reboot	Reboot the system.

Command	Use This Command To
rm	Remove files from your directories.
snmp	Enable or disable SNMP, or change the SNMP port.
snmpaccess	Create, configure, delete, or list SNMP communities.
snmptrap	Create, configure, delete, or list SNMP trap receivers.
sshd	Configure and administer the SSH server.
syslog	Add, delete, or list remote hosts, or restart syslog.
system	Set or display the system configuration, or restart the system interface.
telnetd	Set a Telnet port, enable or disable a Telnet server, show a Telnet port's or Telnet server's configuration, or restart a Telnet port server.
user	Create users and configure privileges, delete users, or list local VCPS users.
version	Display VCPS version information.
view	View the event log and the console port logs.
who	List all users who are currently logged on to the VCPS.

cfg

Configuration database and file manager.

cfg synopsis

```
cfg import [<filename>]
cfg export [<filename>]
cfg save
cfg restore-defaults
cfg load
cfg run [-n]
```

cfg description

The cfg command saves, loads, imports, exports, restores defaults or runs a configuration.

cfg import [<filename>] - Import a configuration from a file. The default name `vcps.cfg` is used if no filename is given.

cfg export [<filename>] - Export the current VCPS configuration to a file. The default name `vcps.cfg` is used if no filename is given.

cfg save - Save the current configuration persistently (from session to session).The previously-saved settings can be retrieved using **`cfg load`**.

cfg restore-defaults - Restore the configuration to factory defaults.

cfg load - Load the saved configuration file from persistent storage.

cfg run - Run the current configuration. This command does not affect the current network settings.

cfg run -n - Run the current configuration including network settings.

cfg examples

- **`cfg run`**
  Run the current configuration except network settings.
- **`cfg save`**
  Save the current configuration.

clear

Clear the event or console logs.

clear synopsis

```
clear eventlog | [portlog <port-number> | <port-name>]
```

clear description

This command allows the user to clear the event log or individual console port logs.

clear options

Clear the non-volatile event log and restart event logging.

```
eventlog
```

Clear the console log for the port number or portname.

```
portlog <port-number> | <port-name>
```

clear examples

- `clear eventlog`
- `clear portlog 14`
- `clear portlog webserv1`

cps

Console port service global configuration command.

cps synopsis

```
cps set baseport <port>
cps set break[n] <break-sequence> <delay>
cps set escapechar <escape-character>
cps set cmdmodechar <command-mode-character>
cps set macro[n] <macro-character> <command>
cps show
cps status users | ports | info
cps connect [<port-number>|<port-name>]
cps disconnect [<user>|@<port-name>|<user>@<port-name>]
cps spy [<port-number>|<port-name>]
cps sendmsg [<user> | @<port-name> | <user>@<port-name>]
<message-text>
cps broadcast <message-text>
```

cps description

The `cps` command configures and administers the console port service.

cps set baseport <port> - Set the TCP base port number for direct console port access.

The default base port number is 9000. It can be set to any unused port from 5000 to 65493. Ports are accessed through either Telnet or SSH using the baseport plus the console port number.

cps set break[n] <break-sequence> <delay> - Set the break sequences for break1 through break9.

The break sequence is a sequence of characters that is sent to the console connection upon request. The delay is the time in milliseconds (ms) for each delay (\d) in the sequence.

The following are special insertable characters:

character	definition
\a	alert
\b	backspace
\d	delay specified for the break sequence.
\f	form-feed
\n	newline
\r	carriage-return
\t	tab
\v	vertical-tab
\z	serial break (hardware break signal)
\\	reverse slant
\^	circumflex
\ooo	octal representation of a character (where ooo is one to three octal digits)
\c	character c (use for '#' character)
^?	delete
^c	control character (c + 0x1f)

cps set escapechar <escape-character> - Set the escape character to access the port server commands while attached to a port. Non-printable control characters must be prefixed with **^**. For example, to set this value to CTRL+A, type **^A**, for the escape character, type **^[**, etc.

cps set cmdmodechar <command-mode-character> - Set the character, while attached to a port, to put the port server in command mode after the escape character has been received.

cps set macro[n] <macro-character> <command> - Define a command macro for macro1 through macro6 that will execute the port server command that is defined by each macro.

- <*macro-character*> is a single character that can be typed instead of both the macro command character and the command.
- <*command*> is the single or two-character port mode command that will be executed by the macro. The port mode commands are:

Character	Definition
.	Disconnect
a	Attach read/write
b	Send broadcast message
c	Toggle flow control
e	Change escape sequence
f	Force attach read/write
L	Toggle logging on/off
l?	Break sequence list
l0	Send default break for port
l1-9	Send specific break sequence

Character	Definition
m	Display the message of the day
p	Redisplay the last 60 lines
r	Redisplay the last 20 lines
s	Spy read only
w	Who is logged on to this console
?	Print this message
<cr>	Ignore/cancel command
^R	Redisplay the last line
\ooo	Send character by octal code

cps show - Display the current configuration.

cps status - Display the console port service status.

cps connect - Start a console session on a port.

cps disconnect - Disconnect a user from a port.

cps spy - Start a read-only session on a port.

cps sendmsg - Send a message to a user.

cps broadcast - Send a message to all users on all active consoles. Enclose the message in quotation marks if spaces are included.

cps examples

- **`cps set basePort 10000`**
  Change the base port to TCP port 10000.
- **`cps set break1 +++\z\d--- 150`**
  Set break1 sequence to **'+++'(hw break)(one delay)'---'.** Set the delay time for this break sequence to 150ms
- **`cps set escapechar ^[`**
  Set break1 sequence to **`<Esc>`**.
- **`cps set macro1 A .`**
  Set macro1 commmand character **`A`** to '**`.`**' (disconnect command). To use, type **`^EA`** (assuming the default escape character **`^E`**).
- **`cps connect 1`**
  Connect to port 1.
- **`cps sendmsg joe@webserv1 "Hello Joe"`**
  Send message to user **`joe`** on console port named **`webserv1`**.
- **`cps sendmsg @dnsserv2 "please note - server going down"`**
  Send a message to the user on port **`dnsserv2`**.

date

Date and time configuration and display.

date synopsis

```
date set [-d mm/dd/yy] [-t hh:mm:ss ] [-z <time-zone>]
date show [-z | timezones]
```

date description

The date command sets and shows the system date, time and time zone configuration.

date set - Set the date, time, and time zone.

date show - Display the current date and time.

date show [timezones | -z] - Display the list of time zones.

date options

Set the system date.

`-d mm/dd/yy`

`--date mm/dd/yy`

Set the system time specified in 24 hour time, <*hours*>:<*minutes*>:<*seconds*>.

`-t hh:mm:ss`

`--time hh:mm:ss`

Set the system time zone in POSIX-style specification.

`-z <time-zone>`

`--zone <time-zone>`

Use `date show timezones` to list valid time zones.

date examples

- **`date set -d 01/01/05 -z CDT`**
  Set the system date to January 1, 2005, central daylight time.
- **`date show`**
  Displays the system's current date and time, and the time zone configuration.
- **`date show timezones`**
  Displays the list of possible time zones:

dhcp

DHCP client configuration and display.

dhcp synopsis

```
dhcp set [-v <vendor-class>] [-c <client-ID>]
[-u <user-class>]
dhcp show
```

dhcp description

The dhcp command sets and shows the system DHCP client configuration.

dhcp set - Set the vendor class, client identifier, and user class.

dhcp show - Display the current DHCP configuration.

dhcp options

Set the DHCP vendor class.

`-v <vendor-class>`

`--vendor <vendor-class>`

Set the DHCP client identifier.

`-c <client-ID>`

`--client <client-ID>`

Set the DHCP user class.

`-u <user-class>`

`--user <user-class>`

dhcp examples

- **`dhcp set -v APC`**
  Set the system DHCP client vendor class to APC.
- **`dhcp show`**
  Shows the current system DHCP client configuration.

exit

Log off the VCPS command line interface.

exit synopsis

```
exit
```

exit description

This command is used to log off the VCPS command line interface.

ftpd

File Transfer Protocol (FTP) server configuration and display.

ftpd synopsis

```
ftpd set -p <port>
ftpd [enable | disable]
ftpd show
```

ftpd description

The ftpd command configures the system FTP server.

ftpd set - Set the FTP server configuration parameters.

ftpd [enable | disable] - Enable or disable the FTP server.

ftpd show - Display the current FTP server configuration.

ftpd options

Set the TCP port that the FTP server will monitor for incoming connections. The port can be from 5000 to 65535. The default port is 21.

```
-p <port>
--port <port>
```

ftpd examples

- **`ftpd set -p 5021`**
  Set the FTP server port to 5021.
- **`ftpd enable`**
  Enable the FTP server.

loadfw

Load and check the VCPS firmware.

loadfw synopsis

```
loadfw [-w] [-c] [-f <info/path> [-p <port>]]
```

loadfw description

The loadfw command updates the VCPS firmware.

loadfw options

Write the firmware update to persistent memory.

`-w`

Check the integrity of the firmware update.

`-c`

Download the firmware update from an FTP server:

`-f <info/path>`

where info <*info/path*> is in the following format:

`username[:password]@host:path`

The TCP port number used by the FTP server.

`-p`

loadfw examples

- **`loadfw -w -f joe@ftpserver:apc_hw10_vcps_101_3.bin`**
  Download the firmware, then write it to persistent memory.
- **`loadfw -c`**
  Check the integrity of the firmware.
- **`loadfw -w`**
  Write the firmware to persistent memory after it has been downloaded.

For details on upgrading VCPS firmware, see Firmware Upgrades.

ls

List files.

ls synopsis

```
ls [files]
```

ls description

This command lists files in the current working directory.

```
ls [files]
```

List the files in the current directory. Wild cards are allowed.

ls examples

- **`ls`**
  List the files in the current directory.
- **`ls cfg`**
  List the files in the user's cfg directory.
- **`ls *.txt`**
  List all files in the current directory that end in ".txt".

network

Configure and display TCP\IP and DNS network parameters.

network synopsis

```
network set [-i <address>] [-n <mask>] [-g <address>]
[-d <name>] [-h <name>] [-b <mode>] [-m <type>]
[-p <address>] [-s <address>]
network show
network status
network restart
```

network description

The network command sets and displays network parameters.

network set - Set network parameters.

network show - Display the current network configuration.

network status - Display the status of the current configuration.

network restart - Restart network services.

network options

Set the IP address of the network interface.

```
-i <address>
--ip <address>
```

Set the network mask.

```
-n <mask>
--netmask <mask>
```

Set the default gateway.

`-g <address>`

`--gateway <address>`

Set the hostname.

`-h <name>`

`--host <name>`

Set which DNS domain to search for unqualified host names.

`-d <name>`

`--domain <name>`

Set the boot mode of the interface to either `static` or `dhcp`. Use static to assign a fixed address. Use DHCP to assign an address using Dynamic Host Configuration Protocol. `dhcp` is enabled by default.

`-b static | dhcp`

`--bootmode static | dhcp`

Set the media type to `10BaseT`, `10BaseT-FDX`, `100BaseTX`, `100BaseTX-FDX`, or `auto`. `auto` is enabled by default.

`-m <type>`

`--media <type>`

Set the primary DNS (Domain Name Server) address. It must be an IP address.

`-p <address>`

`--primaryDNS <address>`

Set a secondary DNS address. It must be an IP address.

`-s <address>`

`--secondaryDNS <address>`

network examples

- **`network show`**
  Display the current network configuration.
- **`network status`**
  Display the current network status.
- **`network set -i 192.168.1.7 -n 255.255.255.255 -g 192.168.1.1 -b static`**
  Set the network address, network mask, default gateway, and bootmode.
- **`network restart`**
  Restart the network services.

ntp

Network Time Protocol client configuration and display.

ntp synopsis

```
ntp set [-p <primary-server>] [-s <secondary-server>]
[-m <minimum-poll-interval>]
[-x <maximum-poll-interval>]
ntp enable
ntp disable
ntp update
ntp show
```

ntp description

This command lets you display and configure the system NTP client settings, perform an update from a configured NTP server, and enable or disable the periodic NTP time update service. By default the NTP service is enabled and time requests will default to public time servers at `pool.ntp.org`. The polling interval options define the polling range intervals from minimum to maximum defined as:

$$\text{time (s)} = (2^{\text{poll interval value}})$$

ntp set - Set the NTP client's primary and secondary servers, and minimum and maximum poll intervals.

ntp enable - Enable the periodic NTP time update service.

ntp disable - Disable the periodic NTP time update service. Users can still use the manual `ntp update` command for one-time updates.

ntp update - Perform an immediate update from the configured primary NTP server.

ntp show - Display the current NTP settings.

ntp options

Set the primary NTP server using an IP address or hostname.

`-p <primary-server>`

`--primary <primary-server>`

Set the secondary NTP server using an IP address or hostname.

`-s <secondary-server>`

`--secondary <secondary-server>`

Set the minimum NTP poll interval.

`-m <minimum-poll-interval>`

`--minpoll <minimum-poll-interval>`

where the minimum poll interval time is $2^{\text{interval seconds}}$ and the minimum value for interval seconds is 4.

Set the maximum NTP poll interval

`-x <maximum-poll-interval>`

`--maxpoll <maximum-poll-interval>`

where the maximum poll interval time is $2^{\text{interval seconds}}$ and the maximum value for interval seconds is 17.

ntp examples

- **`ntp set -p 192.168.0.145 -m 5`**
  Set the primary NTP server to 192.168.0.145 with a minimum poll interval of 32 seconds (2^5).
- **`ntp enable`**
  Enable the NTP service.

ping

ICMP echo command.

ping synopsis

```
ping [ <ip-address> | <hostname> ]
```

ping description

This command sends four ping packets to the specified IP address or DNS hostname and shows the reply statistics for each packet as well as the group of packets.

ping ip-address - Send ping packets to the specified host and display the results.

ping examples

- **`ping www.boingo.com`**
  Ping the host at `www.boingo.com`

port

Serial console port configuration and display command.

port synopsis

```
port set <port>[-<port>][,<port>] [-b <baudrate]
[-p <parity>] [-f <flowctrl>] [-o <options>]
[-n <port-name>] [-m <motd>] [-t <idletimeout>]
[-i <idlestring>] [-k <break-seq-number>]
[-a <access-mode>] [-l <logging>]

port show <port>

port list
```

port description

The port command is used to configure and display the name and serial communication parameters for the VCPS serial ports. Ports can be specified by their number or configured name, either singly, individually as a comma separated list (1,5,12), or as a range (10-15). These can also be combined (1,3,5-15).

port set <port> [-b <baudrate>] - Set the baudrate for the specified port. Baudrate values are `300`, `600`, `1200`, `1800`, `2400`, `4800`, `9600`, `19200`, `38400`, `57600`, or `115200`.

port set <port> [-p <parity>] - Set the parity for the specified port. Parity values are `none`, `mark`, `even`, `odd` or `space`.

port set <port> [-f <flow-control>] - Set the flow control parameters. This value is specified as a plus sign-separated (+) list of options. The flow-control options are:

- `ixon` - Enable XON/XOFF flow control on output
- `ixany` - Enable any character to restart output
- `ixoff` - Disable XON/XOFF flow control on input
- `crtscts` - Enable RTS/CTS (hardware) flow control

port set <port> [-o <options>] - Set the port communication options. This value is specified as a plus sign-separated (+) list of options. Port communication options are:

- `cstopb` - Set two stop bits instead of one.
- `hupcl` - Lower modem control lines after the last process closes the device (hangs up).
- `striphigh` - Remove the high bit from all data coming from this console and all clients connected to this console before processing.

port set <port> [-n <port-name>] - Set the name of the specified port.

port set <port> [-m <motd>] - Set the message of the day that will be displayed when a user logs into the port.

port set <port> [-t <idletimeout>] - Set the idle timeout for the port.

port set <port> [-i <idlestring>] - Set the string to be sent to the port after the idle timeout has expired.

port set <port> [-k <break-seq-number>] - Set the break sequence sent with the '`l0`' port mode command.

port set <port> [-a <accessmode>] - Set the remote access mode for this port to either Telnet or SSH.

port set <port> [-l [enabled | disabled]] - Enable or disable logging on this port.

port show <port> - Show the current configuration of this port.

port list - List all ports.

port options

Set the baud rate for the specified port.

`-b <baudrate>`

`--baud <baudrate>`

Set the parity for the specified port.

`-p <parity>`

`--parity <parity>`

Set the flow control for the specified port.

`-f <flowcontrol>`

`--flowctrl <flowcontrol>`

Set the options for the specified port.

`-o <options>`

`--options <options>`

Set the name of the specified port.

`-n <port-name>`

`--name <port-name>`

Set the message of the day for the specified port. Use quotes to enclose anything with spaces.

`-m <message>`

`--motd <message>`

Set the idle timeout for the specified port.

`-t <idletimeout>`

`--idletimeout <idletimeout>`

Set the idle timeout string for the specified port.

`-i <idlestring>`

`--idlestring <idlestring>`

Set the break sequence number for the specified port.

`-k <break-seq-number>`

`--breakseq <break-seq-number>`

Set the remote access mode for the specified port to either Telnet or SSH.

`-a <access-mode>`

`--access <access-mode>`

Enable or disable logging for the specified port.

`-l [enable | disable]`

`--logging [enable | disable]`

port examples

- **`port set 1 --name webserver1`**
  Set the name of port number 1 to **`webserver1`**.
- **`port set webserver1 -k break2`**
  Set the break sequence of the port named `webserver1` to break sequence 2.

For more information on break sequences, see the cps command.

- **`port set 2 -o cstopb+hupcl`**
  Set the options for port 2 to use two stop bits, lower the modem control lines after hang up, and NOT remove the high bit from incoming data.
- **`port set 10 -l enabled`**
  Enable logging on port 10.
- **`port show webserver1`**
  Display the current configuration of the port named **`webserver1`**.

prompt

Command prompt form.

prompt synopsis

```
prompt [short|long]
```

prompt description

This command sets the command prompt to either the short or long form. The short form shows the configured host name as the prompt in the format *hostname*>. The long form shows the user currently logged in for the session and the configured hostname in the format *user@hostname*>.

For more information on configured host names, see the network command

The prompt notifies the user if there are unsaved configuration changes with the string `[s!]` prepended to the prompt in short form, or the string `[save cfg!]` prepended to the prompt in long form.

The prompt also notifies the user if any services need to be restarted for changes to take effect. This is shown in the short form by the prepended string `[r!]` and in long form by the prepended string `[run cfg!]`.

prompt short - Set the prompt to short form.

prompt long - Set the prompt to long form.

prompt examples

- prompt short
- prompt long

radius

RADIUS client configuration and display.

radius synopsis

```
radius set <server> [-h <host-address>] [-p <port>]
[-s <shared-secret>] [-t <timeout>] [-r <retries>]
radius show
```

radius description

This command is used to configure the RADIUS client on the VCPS.

radius set <server> - Configure the RADIUS client parameters for the specified server. *<server>* is either the primary or secondary RADIUS server and may be specified by name (primary or secondary) or by number (1 or 2).

radius show - Display the current configuration of the RADIUS client.

radius options

Set the IP address of the specified RADIUS server using an IP address or hostname.

`-h <host-address>`

`--host <host-address>`

Set the UDP port to communicate with the specified RADIUS server.

`-p <port>`

`--port <port>`

Set the shared secret to use for the specified RADIUS server.

`-s <shared-secret>`

`--secret <shared-secret>`

Set the amount of time, in seconds, to wait for a response from the specified RADIUS server.

`-t <timeout>`

`--timeout <timeout>`

Set the number of retries to attempt to contact the RADIUS server before failing a login authentication. If authentication is set up as `radius_then_local`, the local user database will perform the authentication.

`-r <retries>`

`--retries <retries>`

radius examples

- **`radius set primary -p 9202`**
  Communicate with the primary RADIUS server on the non-standard TCP port 9202.
- **`radius set 2 --host 192.168.0.13`**
  Set the address on the secondary RADIUS server to 192.168.0.13.
- **`radius set 1 -t 5 -r 3`**
  Timeout after waiting 5 seconds for a response from the primary server, and make 3 retries before failing.
- **`radius show`**
  Display the current RADIUS client configuration.

reboot

Reboot the system.

reboot synopsis

```
reboot
```

reboot description

Reboot the VCPS.

rm

Remove files

rm synopsis

```
rm <files>
```

rm description

This command deletes files from the user's directories.

rm <files> - Delete the specified files. Wild cards are allowed.

rm examples

- **`rm *`**
  Delete all files in the current directory.
- **`rm cfg/*.cfg`**
  Delete all files in the cfg directory that end with `*.cfg`.

snmp

SNMP agent configuration and display.

snmp synopsis

```
snmp set -p <port>
snmp [enable | disable]
snmp show
```

snmp description

This command configures and administers the VCPS SNMP server.

snmp set - Configure the SNMP server's parameters.

snmp enable - Enable the SNMP server.

snmp disable - Disable the SNMP server.

snmp show - Display the SNMP server's current configuration.

snmp options

Sets the SNMP server UDP listening port.

```
-p <port>
--port <port>
```

snmp examples

- **`snmp set -p 9005`**
  Set the SNMP server to listen on port 9005 for any SNMP requests.
- **`snmp enable`**
  Enable the SNMP server.

snmpaccess

SNMP community configuration and display.

snmpaccess synopsis

```
snmpaccess [add | set] <community> [-a <rw-access>]
[-f <address-filter>]
snmpaccess del <community>
snmpaccess show <community>
snmpaccess list
```

snmpaccess description

This command configures the VCPS SNMP access communities for the SNMP server.

snmpaccess add <community> - Create a new SNMP access community. The default value for access is read-only and for address filters is 0.0.0.0/0.

snmpaccess set <community> - Edit the configuration for the specified SNMP community.

snmpaccess del <community> - Remove an SNMP community from the list of communities.

snmpaccess show <community> - Display the configuration of the specified SNMP community.

snmpaccess list - List all the configured SNMP access communities.

snmpaccess options

Set the access rights for the specified community.

- r - read-only
- w - read-write
- disabled - disable access for this community.

`-a r | w | disabled`

`--access r | w | disabled`

Set the range of device addresses that may access the specified community. The address filter is specified as a standard IP address mask.

`-f <address-filter>`

`--filter <address-filter>`

snmpaccess examples

- **`snmpaccess add private`**
  Add an SNMP community named `private` to the list of access communities. If you do not define access rights and a range of device addresses that may access the community, the default settings (read-only and no address-filter) are applied.
- **`snmpaccess set private -a w -f 192.168.0.0/24`**
  Edit the configuration of the SNMP community named `private` to be `read-write`, and allow access to any device on the 192.168.0 network segment.
- **`snmpaccess del public`**
  Deletes the SNMP community named `public`.

For information on access filter values, see SNMP.

snmptrap

SNMP trap receivers configuration and display.

snmptrap synopsis

```
snmptrap [add | set] <trap-receiver> [-c <community>]
[-g <generate>] [-a <authgenerate>]
snmptrap [show | del] <trap-receiver>
snmptrap list
```

snmptrap description

This command configures the SNMP trap receivers that will receive traps from the VCPS. The trap receiver is a single host, specified as an IP address or host name.

snmptrap add <trap-receiver> - Add the specified device to the list of trap receivers.

snmptrap set <trap-receiver> - Edit the configuration of the specified trap receiver.

snmptrap show <trap-receiver> - Display the current configuration of a single trap receiver.

snmptrap del <trap-receiver> - Remove the specified trap receiver.

snmptrap list - List all the configured SNMP trap receivers.

snmptrap options

Set the community name for the specified trap receiver to receive traps on.

```
-c <community>
--community <community>
```

Enable or disable trap generation for the specified trap receiver.

`-g <generate>`

`--generate <generate>`

Enable or disable whether the specified trap receiver will receive authentication failure traps from the VCPS.

`-a <authgenerate>`

`--authenticate <authgenerate>`

snmptrap examples

- **`snmptrap add 192.168.1.45`**
  Add the device at 192.168.1.45 to the list of trap receivers with all default configuration values.
- **`snmptrap set 192.168.1.45 -c localprivate -g enabled -a disabled`**
  Edit the configuration of the trap receivers at 192.168.1.45 to receive traps on the community `localprivate`, enable trap generation, and disable authentication traps.

sshd

Secure shell server (SSH v1 and SSHv2) configuration and display.

sshd synopsis

```
sshd set [-p <port>] [-c <sshv2-ciphers>]
[-C <sshv1-ciphers>] [-v <ssh-version>]

sshd [enable | disable]

sshd show

sshd keygen -s <key-size>
```

sshd description

Use this command to configure and administer the SSH server.

sshd set - Configure the SSH server's parameters. By default, the SSH server is enabled and uses SSH version 2 with 3DES and Blowfish ciphers.

sshd enable - Enable the SSH server.

sshd disable - Disable the SSH server.

sshd show - Display the SSH server's current configuration.

ssh keygen - Generate a new SSH key.

sshd options

Set the TCP port for the SSH server.

`-p`

`--port`

Set the SSH version 2 ciphers to use. This value is specified as a list of ciphers separated by a plus (+) sign. Acceptable values are 3des, blowfish, aes128, and aes256. Leaving a cipher out of the list will disable it.

`-c <sshv2-ciphers>`

`--v2ciphers <sshv2-ciphers>`

Set the SSH version 1 ciphers to use. This value is specified as a list of ciphers separated by a plus (+) sign. Acceptable values are des and blowfish. Leaving a cipher out of the list will disable it.

`-C <sshv1-ciphers>`

`--v1ciphers <sshv1-ciphers>`

Sets the SSH server to use either SSH version 1 or 2.

`-v 1 | 2`

`--version 1 | 2`

Generate the new SSH key with a specific key size of 768, 1024, 2048, or 4098 bits.

`-s <key-size>`

sshd examples

- **`sshd set -C blowfish -v 1`**
  Set the SSH server to use the Blowfish cipher only and use SSH version 1.
- **`sshd set -c blowfish+aes256 --version 2`**
  Set the SSH server to use SSH version 2 with the version 2 ciphers Blowfish and AES256.
- **`sshd keygen -s 2048`**
  Generate a new 2048-bit SSH key.

syslog

Syslog messaging recipient configuration and display.

syslog synopsis

```
syslog [add | del] <remote-host>
syslog list
```

syslog description

Use this command to configure the list of remote syslog servers that will receive syslog messages from the VCPS. The remote host may be specified as an IP address or DNS hostname.

syslog add <remote-host> - Add a new remote syslog server to the list.

syslog del <remote-host> - Remove a remote syslog server from the list.

syslog list - List all configured remote syslog servers.

syslog examples

- **`syslog add 192.168.1.123`**
  Add the remote syslog server at 192.168.1.123 to the list of syslog servers.
- **`syslog del server1.mydomain.com`**
  Remove the server `server1.mydomain.com` from the list of syslog servers.

system

Configure global system and SNMP MIB II parameters

system synopsis

```
system set [-n <system-name>] [-c <system-contact>]
[-l <system-location>] [-a <authentication-type>]
system [show | restart]
```

system description

This command lets you configure the global system parameters and restart the system.

system set - Configure the system parameters.

system show - Display the current system configuration.

system restart - Restart the system.

system options

Set the global system name. The default is `unknown`. The maximum length is 256 characters.

`-n <system-name>`

`--name <system-name>`

Set the contact information for the administrator of this VCPS. The default is `unknown`. The maximum length is 256 characters.

`-c <system-contact>`

`--contact <system-contact>`

Set the user-specified location information for this VCPS. The default is `unknown`. Maximum length is 256 characters.

`-l <system-location>`

`--location <system-location>`

Set the authentication method used to validate user access for telnet and ssh. Values are `local`, `radius`, `local_then_radius`, or `radius_then_local`. The default is `local`.

`-a <authentication-type>`

`--authtype <authentication-type>`

system examples

- **`system set -n "VCPS Rack 2"`**
  Set the system name to `VCPS Rack 2`.
- **`system set -c "John Smith - (518) 555-5555 x1234"`**
  Set the system contact information to `John Smith - (518) 555-5555 x1234`.
- **`system set -a radius_then_local`**
  Set the system to validate users by using RADIUS first, then local authentication if RADIUS fails.

telnetd

Telnet server configuration and display.

telnetd synopsis

```
telnetd set [-p <port>]
telnetd [enable | disable | show]
```

telnetd description

This command lets you configure the Telnet server on the VCPS.

telnetd set - Configure the Telnet server parameters.

telnetd enable - Enable the Telnet server.

telnetd disable - Disable the Telnet server.

telnetd show - Display the Telnet server current configuration.

telnetd options

Set the TCP port that the Telnet server will monitor. Choose port numbers from 5000 to 65535. The default is 23.

```
-p <port>
--port <port>
```

telnetd examples

- **`telnetd set -p 5023`**
  Configure the Telnet server monitor port 5023.

user

User management and display.

user synopsis

```
user [add | set] <username> [-p <password>] [-a <access-rights>]
user perm-admin [-n <perm-admin-name>] [-p <password>]
user [show | del] <username>
user [status | list]S
```

user description

This command is used to configure the users and their access rights.

user add <username> - Add a new user to the system.

user set <username> - Configure a user's password and access rights.

user perm-admin - Configure the user name and password of the permanent administrative user.

user show <username> - Show the specified user's configuration

user del <username> - Remove a user from the system.

user status - Show all users that are currently logged onto the system.

user list - Display a list of all system users.

user options

Set the name of the permanent system administrative user. The default value is apc. The maximum length is 32 bytes.

```
-n <perm-admin-name>
```

`--name <perm-admin-name>`

Set the password for the specified user. The maximum length is 32 bytes.

`-p <password>`

`--password <password>`

Select from the following access rights for the specified user:

- **`admin`**: Can configure all VCPS network and system parameters, and connect to all VCPS ports.
- **`port-admin`**: Can configure all VCPS port parameters and access all ports.
- **`port-readonly`**: Can view some port parameters but does not have write access. This user cannot connect to a port.
- **`<ports>:<access>`**: Port users are assigned permissions on a per port basis. They can monitor port activity (m) or they can monitor and access assigned ports (a). A port user can monitor or access multiple ports. Ports can be assigned by port number, port name, or as a range of ports. A port user can be assigned to monitor some ports and have access to others.

  `-a <access-rights>`

  `--access <access-rights>`

user examples

- **`user add joe -p joespassword -a port-admin`**
  Add the user named `joe` to the system with the password `joespassword`, and set his access rights to `port-admin`.
- **`user set mike -a port1,5-7:m;port10,12:a`**
  Set the access rights for the user named `mike` so that this user can monitor ports 1,5,6,7, and can access ports 10,12.
- **`user perm-admin -n john -p johnsnewpassword`**
  Set the permanent administrative user name to `john` and set the password to `johnsnewpassword`.

version

Show the current firmware version information for the VCPS.

version synopsis

```
version
```

version description

This command displays the current version of the firmware running on the VCPS.

view

View syslog and console logs.

view synopsis

```
view events
view log [<port-name>|<port-number>]
view list
```

view description

Use this command to view logs that are stored by the system.

view events - View the event log.

view log <port> - View individual console traffic logs. The port is specified as either a number (1-42) or by the name of the port.

For more information on ports, see the port command.

view list - Display a list of all the console logs.

view examples

- **`view log 19`**
  Display the traffic log for console port 19.
- **`view log webserver1`**
  Display the traffic log for the console port named `webserver1`.

who

Show users that are currently logged in.

who synopsis

```
who
```

who description

This command displays a list of all users who are currently logged onto the system.

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the VCPS is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Summary of access methods

Serial control console.

Security Access	Description
Access is by user name and password. • Local or RADIUS authentication	Always enabled.

Remote control console.

Security Access	Description
• User name and password • Local or RADIUS authentication • Configurable server port • Server Enable/Disable • Secure SHell (SSH)	For high security, use SSH. • With Telnet, the user name and password are transmitted as plain text. • SSH provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission. • If you choose SSH as your remote console protocol, you should disable Telnet for a higher level of security.

SNMP.

Security Access	Description
• Community Name • DNS Host filters • NMS IP filters • Agent Enable/Disable • 20 access communities with read/write/disable capability	The DNS Host filters restrict access only to the NMS at that location, and the NMS IP filters allow access only from designated IP addresses. • 162.245.12.1 allows only the NMS with that IP address to have access. • 162.245.12.0/24 allows access for any NMS on the 162.245.12 segment. • 162.245.0.0/16 allows access for any NMS on the 162.245 segment. • 162.0.0.0/8 allows access for any NMS on the 162 segment. • 0.0.0.0/0 allows access for any NMS.

File transfer protocols.

Security Access	Description
• User name and password • Local or RADIUS authentication • Configurable server port • Server Enable/Disable • Secure CoPy (SCP)	With FTP, the user name and password are transmitted as plain text, and files are transferred without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP.

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the VCPS, immediately change the default user name and password. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If the Telnet, FTP, or SSH/SCP server uses a non-standard port, a user must specify the port when connecting to the VCPS. The non-standard port address becomes an extra “password,” hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard “well known ports” for the protocols. To hide the interfaces, use any port numbers from 5000 to 65535.

User names, passwords, community names (SNMP)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the control console of the VCPS. If your network requires the higher security of the encryption-based options available for the control console, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Security Protocols

Overview

You can select to use the basic security features for the VCPS that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

To ensure that data and communication between the VCPS and the control console cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- To encrypt user names, passwords, and all communication for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure CoPy (SCP) protocol.

For more information on these protocols for encryption-based security, see Secure SHell (SSH) and Secure CoPy (SCP).

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the VCPS) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from anyone intercepting network traffic.
- To authenticate the SSH server (the VCPS) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.
- The VCPS supports versions 1 and 2 of SSH.
- If you enable SSH, you should disable Telnet for a higher level of security for your system.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.

For information on supported SSH client applications, see Telnet and SSH.

Secure CoPy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- If you enabled SSH and SCP, you should disable FTP for a higher level of security for your system.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service. Use this option to centrally administer remote access for each VCPS port.

When a user accesses the VCPS, an authentication request is sent to the RADIUS server to determine the user's permission level.

RADIUS user names are limited to 32 characters.

For more information on user permission levels, see User Management

Configuring the RADIUS server

You must configure your RADIUS server to work with the VCPS.

For details on how to set the RADIUS parameters, see radius.

1. Define the APC vendor identifier in your RADIUS server. 318 is the APC Private Enterprise Number assigned by the Internet Assigned Numbers Authority (IANA).
2. Define a RADIUS vendor-specific attribute called APC-Permissions. This is a string with an attribute identifier of 3.

3. Configure RADIUS users.

RADIUS user names are limited to 32 characters.

The APC-Permissions attribute must be configured for each administrator, port administrator, and read-only user accessing the VCPS. The APC-Permissions attribute is a string and is set as follows:

`CPS_PERMS=admin`

`CPS_PERMS=` identifies these as console port server permissions. `admin` is a user permission string.

For more information on user permission levels, see User Management.

Permissions for individual ports can be configured using the vendor-specific APC-PERM attribute or the standard RADIUS NAS-Port attribute.

APC-PERM attribute. To allow a user to access a port, set the APC-PERM attribute as follows:

`CPS_PERMS=port1:ma`

`CPS_PERMS=` identifies these as console port server permissions. `port1:ma` is a user permission string.

NAS-Port attribute. The Network Access Server Port (NAS-Port), RADIUS attribute ID 5 as defined in **RFC 2865**, can be used to assign per port permissions for a user. Specifying a port using NAS-Port grants a user both read and write access to the specified port. For example, the attribute NAS-Port=1 is equivalent to using the vendor-specific attribute APC-Permissions="CPS_PERMS=1:ma".

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Events and Event Log

Overview

The Vertical Console Port Server logs syslog messages and SNMP MIB II traps for selected events. These events are stored in a local event log and in up to 20 remote syslog servers.

Using the CLI, you can add or delete a remote syslog server, or display a list of remote servers configured to receive messages from VCPS.

For details on how to use the syslog command in the CLI, see syslog.

Accessing the Event Log

The event log can be accessed using one of these methods:

- Direct viewing from within the CLI using the `view eventlog` command
- Offline viewing by transferring the file from the VCPS using either FTP or SCP. The event log is stored as `/logs/messages` in the file system.

Note

You must be an administrator to use FTP and SCP to access the event log.

The following table lists the events that are logged by VCPS. All events will be sent to remote syslog servers. SNMP traps are sent for MIB II traps only.

Event	Definition
warmStart †	The VCPS is reinitializing and its configuration may change.
coldStart †	The VCPS is reinitializing and its configuration will not change.
reboot	The VCPS will shut down and restart its services.
shutdown	The VCPS will shut down but will not automatically restart.
network up †	One of the VCPS network interfaces has been accessed.
network down †	One of the VCPS network interfaces has shut down.
password changed	The user whose login is displayed has set a new password.
user logged in	The user whose login is displayed has logged on to VCPS.
user logged out	The user whose login is displayed has logged off from VCPS.
unauthorized access attempt	An unauthorized user attempted to access the VCPS.
file transfer started/finished	A file (new firmware or a configuration file, for example) has been uploaded to the VCPS.
user port access	A user has accessed one of the VCPS server serial ports. The login, port number, and port name are displayed.
† This event generates an SNMP MIB II trap.	

Firmware Upgrades

Overview

The VCPS supports upgradable firmware using binary firmware files provided by APC either through the internet or on CD. Each of these files contains protection mechanisms to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the VCPS, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to VCPSs.

To transfer a firmware file to a VCPS, see Upgrading Firmware.

To verify a file transfer, see Verifying upgrades and updates.

Upgrading Firmware

Benefits of upgrading firmware

Upgrading the firmware on the VCPS has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all VCPSs support the same features in the same manner.

Firmware files (VCPS)

A firmware version for the VCPS uses the following basic format:

`apc_hwx_vcps_version_build.bin`

- **`apc`**: Indicates that this is an APC file.
- **`hwx`**: Identifies the version of the VCPS hardware that will run this binary file.
- **`vcps`**: Identifies the application as being for the VCPS.
- ***`version`***: The version number of the application file. For example, a code of 100 would indicate version 1.0.0.
- ***`build`***: The build number of the application file. For example, a code of 623 would indicate build number 623.
- **`bin`**: Indicates that this is a binary firmware image.

Obtain the latest firmware version

You can obtain the firmware you need for a firmware upgrade from the download section of the APC Web site **www.apc.com/tools/download**.

Firmware file transfer methods

You can transfer the latest firmware to a VCPS using one of the following methods:

- Upload the firmware to a VCPS using FTP or SCP.
- Download the firmware from an FTP server (if your company or agency has a centralized FTP server from which to obtain firmware).

Instructions for using FTP or SCP. For you to be able to use FTP or SCP to upgrade a single VCPS over the network:

- The VCPS must be connected to the network.
- The FTP or SSH server must be enabled at the VCPS.
- The VCPS must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

Upload firmware to a VCPS

To upload firmware to a VCPS after you download it from the APC Web site:

1. Open a command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory `C:\apc`, the commands would be those shown in **bold**:

   ```
   C:\>cd apc
   C:\apc>dir
   ```

   The file listed for a VCPS, for example, might be the following:

   ```
   –apc_hw10_vcps_100_623.bin
   ```

    To use SCP, skip to step 7.

2. Open an FTP client session:

   ```
   C:\apc>ftp
   ```

3. Type `open` and the VCPS's IP address, and press ENTER. If the **Port** setting for **FTP Server** has changed from its default of **21**, you must use the non-default value in the FTP command.
   a. For some FTP clients, use a colon to add the port number to the end of the IP address.
   b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the VCPS's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to a VCPS with an IP address of 150.250.6.10.
   ```
   ftp> open 150.250.6.10 21000
   ```
4. Log on using an Administrator user name and password. (**apc** is the default for both.)
5. The firmware image file must be transferred to the local firmware directory named `firmware`. The file must be renamed `vcps.bin`. For example:
   ```
   ftp> bin
   ftp> cd firmware
   ftp> put apc_hw10_vcps_100_623.bin vcps.bin
   ```
6. When FTP confirms the transfer, type `quit` to close the session.

Go to Step 8.

To use Secure CoPy (SCP) to upgrade the firmware:

7. Use an SCP command line to transfer the firmware module to the VCPS. The following example assumes a VCPS IP address of 158.205.6.185, and a firmware module of **apc_hw10_vcps_100_623.bin**.
   ```
   scp apc_hw10_vcps_100_623.bin apc@158.205.6.185:/
   firmware/vcps.bin
   ```
8. In the control console, enter `loadfw -c` to make sure the image is a

valid VCPS firmware image. After checks have been performed, an MD5 hash is displayed. This MD5 hash must match the MD5 hash from the .md5 file that accompanied the firmware image file.

9. In the control console, enter `loadfw -w` to write the firmware image to the VCPS flash memory.
10. Enter `reboot` to have your changes take effect.

Download firmware from an FTP server

To download firmware from an FTP server:

1. In the control console, enter this command:
   `loadfw -f username[:password]@host:path [-p <portnum>]`
   This starts the FTP client on the VCPS and downloads the firmware to `/firmware/vcps.bin` on the VCPS.
2. IIn the control console, enter `loadfw -c` to make sure the image is a valid VCPS firmware image. After checks have been performed, an MD5 hash is displayed. This MD5 hash must match the MD5 hash from the .md5 file that accompanied the firmware image file.
3. In the control console, enter `loadfw -w` to write the firmware image to the VCPS flash memory.
4. Enter `reboot` to have your changes take effect.

In the following example:

```
loadfw -w -f mtsmith@158.215.7.30:/apc/apc_hw10_vcps_100_623.bin
```

- **`mtsmith`** is the username to access the FTP server (you will be prompted for a password)
- **`158.215.7.30`** is the IP address of the FTP server. You could also use DNS hostname.
- **`/apc`** is the directory path on the server
- **`apc_hw10_vcps_100_623.bin`** is the downloadable firmware

– The **-w** option writes the file to flash memory after downloading and verifying the file image.

Verifying upgrades and updates

To verify that the firmware upgrade was successful, use an SNMP GET to the MIB II **sysDescr** OID.

Product Information

Warranty and Service

Limited warranty

APC warrants the VCPS to be free from defects in materials and workmanship for a period of WARRANTY LENGTH from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

To obtain support for problems with your VCPS:

1. Note the serial number and date of purchase. For a separately shipped Management Card, the serial number is on the card itself. For a UPS with a pre-installed or embedded card, note the serial number of the UPS itself.
2. Contact Customer Support at a phone number listed under APC Worldwide Customer Support at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

The VCPS is sensitive to static electricity. When handling the VCPS, touch only the end plate while using one or more of these electrostatic-discharge devices (ESDs): wrist straps, heel straps, toe straps, or conductive shoes.

Recycling the Battery

The VCPS contains a removable, lithium coin-cell battery. When discarding this battery, you must follow local rules for recycling.

Life-Support Policy

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

Specifications

Electrical

Item	Specification
Acceptable input voltage	19–30 VDC
Maximum total current draw	110 mA
Output relay contact rating	1A @ 30V

Physical

Item	Specification
Size (H × W × D)	1.46 × 4.75 × 4.3 in (3.7 × 12.1 × 10.9 cm)
Weight	0.25 lb (0.11 kg)
Shipping weight	0.8 lb (0.36 kg)

Index

R

S

T

U

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)

    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**

    Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
  - Regional centers:

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Copyright

This product includes firmware with the following copyrights and attributions:

990-2190B 1/2005