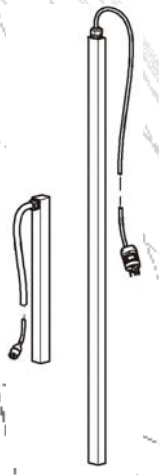
User Guide

Metered Rack Power Distribution Unit

AP88XX



Contents

Introduction 1

Product Features. 1

Access Priorities for Logging on. 2

Types of User Accounts 2

Watchdog Features. 3

Overview 3
Network interface watchdog mechanism 3
Resetting the network timer 3

Network Port Sharing 3

About the Network Port Sharing Feature 3
Display ID 3
Installation Instructions 3

Getting Started 4

Establish Network Settings 5

TCP/IP configuration methods 5
INI file utility 5
DHCP and BOOTP configuration 5
Command Line Interface 7

Recovering from a Lost Password 8

Rack PDU Front Panel 9

Display Tree Example 1 11
Display Tree Example 2 12
Network Status LED 13
10/100 LED 13
Load indicator LED 13

Command Line Interface 14

About the Command Line Interface 14

Log on to the Command Line Interface 14
Remote access to the command line interface 14
Local access to the command line interface 15
About the Main Screen 15
Using the Command Line Interface 16
Command Syntax 17
Command Response Codes 18
Network Management Card Command Descriptions 19
about 19
alarmcount 19
boot 20
cd 20
clrrst 20
console 21
date 22
delete 22
dir 22
dns 23
eventlog 23
exit 23
format 23
FTP 24
help 24
netstat 24
ntp 24
ping 25
portSpeed 25
prompt 25
quit 25
radius 26
reboot 26
resetToDef 27
snmp, snmpv3 27
system 27
tcpip 28
tcpip6 28
user 29
web 29
xferINI 30
xferStatus 30

Device Command Descriptions 31
Network Port Sharing Commands 31
bkLowLoad 31
bkNearOver 31
bkOverLoad 32
bkReading 32
devLowLoad 32
devNearOver 33
devOverLoad 33
devReading 33
humLow 34
humMin 34
humReading 34
phLowLoad 35
phNearOver 35
phOverLoad 35
phReading 36
prodInfo 37
sensorName 37
tempHigh 38
tempMax 38
tempReading 38
whoami 39

Web Interface 40

Supported Web Browsers 40

Logging On to the Web Interface 40
Overview 40
URL address formats 41

Web Interface Features 42
Tabs 42
Device status icons 42
Quick Links 43
Other Web interface features 43

Network Port Sharing on the Web Interface 44
Group Control using Network Port Sharing 44

About the Home Tab 46
The Overview view 46
The Alarm Status view 46

Device Management 47

About the Device Manager Tab 47

Viewing the Load Status and Peak Load 47

Configuring Load Thresholds 47

Configure the Name and Location of the Rack PDU 48

Resetting Peak Load and kWh. 48

Environment 49

Configure Temperature and Humidity Sensors 49

Logs 50

Use the Event and Data Logs. 50

Event log 50
Data log 52
How to use FTP or SCP to retrieve log files 54

Administration: Security 55

Local Users 55

Setting user access 55

Remote Users 55

Authentication 55
RADIUS 56

Configure the RADIUS Server 57

Summary of the configuration procedure 57
Configuring a RADIUS server on UNIX® with shadow passwords 57
Supported RADIUS servers 57
RADIUS and Network Port Sharing 57

Inactivity Timeout 58

Administration: Network Features 59

TCP/IP and Communication Settings 59

TCP/IP settings 59
DHCP response options 60

Port Speed 61
Ping Response 61
DNS. 62
Web. 63
Console 64
SNMP 65
SNMPv1 66
SNMPv3 67
FTP Server 68
Administration: Notification 69
Event Actions 69
Types of notification 69
Configuring event actions 69
Active, Automatic, Direct Notification. 71
E-mail notification 71
SNMP traps 73
SNMP Trap Test 73
Remote Monitoring Service 74
Syslog 74
Administration: General Options 76
Identification 76
Set the Date and Time. 76
Mode 76
Daylight saving 77
Format 77
Use an .ini File 77
Event Log and Temperature Units. 78
Color-code event log text 78
Change the default temperature scale 78
Reset the Rack PDU 78
Configure Links. 79
About the Rack PDU 79

Device IP Configuration Wizard 80

Capabilities, Requirements, and Installation 80

How to use the Wizard to configure TCP/IP settings 80
System requirements 80
Installation 80

Use the Wizard 80

Launch the Wizard 80
Configure the basic TCP/IP settings remotely 80
Configure or reconfigure the TCP/IP settings locally 81

How to Export Configuration Settings 82

Retrieving and Exporting the .ini File 82

Summary of the procedure 82
Contents of the .ini file 82
INI and Network Port Sharing 82
Detailed procedures 83

The Upload Event and Error Messages 85

The event and its error messages 85
Messages in config.ini 85
Errors generated by overridden values 85

Related Topics 85

File Transfers 86

How to Upgrade Firmware 86

Benefits of upgrading firmware 86
Firmware module files (Rack PDU) 86

Firmware File Transfer Methods 86

Using the Firmware Upgrade Utility 87
Use FTP or SCP to upgrade one Rack PDU 87
Use XMODEM to upgrade one Rack PDU 88
How to upgrade multiple Rack PDUs 89
Using the Firmware Upgrade Utility for multiple upgrades 89
Using a USB flash drive to upgrade one Rack PDU 89

Verifying Upgrades and Updates 91

Verify the success or failure of the transfer 91
Last Transfer Result codes 91
Verify the version numbers of installed firmware. 91

Troubleshooting 92

Rack PDU Access Problems 92

Appendix A: List of Supported Commands 93

Network Management Card Command Descriptions 93
Device Command Descriptions 95

Introduction

Product Features

The APC by Schneider Electric Metered Rack Power Distribution Unit (PDU) may be used as a stand-alone, network-manageable power distribution device or up to 4 devices can be connected together with one network connection. The Rack PDU provides real-time remote monitoring of connected loads. User-defined alarms warn of potential circuit overloads.

Your unit comes with one terminator installed. It is not needed for stand-alone operation of this unit. To use Network Port Sharing between up to four units, a terminator must be installed in the In port at one end of the group and another on the Out port at the other end of the group.

You can manage a Rack PDU through its Web interface, its command line interface (CLI), StruxureWare, or Simple Network Management Protocol (SNMP). (To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, available at **www.apc.com**.) Rack PDUs have these additional features:

- Peak load, and power and energy monitoring for all connected loads.
- Voltage, current, and power monitoring for phases.
- Current monitoring for outlet banks.
- Configurable alarm thresholds that provide network and visual alarms to help avoid overloaded circuits.
- Three levels of user access accounts: Administrator, Device User, and Read-Only User.
- Event and data logging. The event log is accessible by Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), serial connection, or Web browser (using HTTPS access with SSL, or using HTTP access). The data log is accessible by Web browser, SCP, or FTP.
- E-mail notifications for Rack PDU and system events.
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level or category of the Rack PDU and system events.
- Security protocols for authentication and encryption.
- Network Port Sharing: Up to four Rack PDUs can be connected using the In and Out ports so that only one network connection is necessary.

Note: The Rack PDU does not provide power surge protection. To ensure that the device is protected from power failure or power surges, connect the Rack PDU to an APC Uninterruptible Power Supply (UPS).

Access Priorities for Logging on

Only one user at a time can log on to the Rack PDU. The priority for access, beginning with the highest priority, is as follows:

- Local access to the command line interface from a computer with a direct serial connection to the Rack PDU
- Telnet or Secure SHell (SSH) access to the command line interface from a remote computer
- Web access, either directly or through StruxureWare Data Center Expert

  Note: See “SNMP” on page 65 for information about how SNMP access to the Rack PDU is controlled.

Types of User Accounts

The Rack PDU has three levels of access (Administrator, Device User, and Read-Only User), which are protected by user name and password requirements.

- An Administrator can use all of the menus in the Web interface and all of the commands in the command line interface. The default user name and password are both **apc**.
- A Device User can access only the following:
  - In the Web interface, the menus on the **Device Manager** tab, the **Environment** tab, and the event and data logs, accessible under the **Events** and **Data** headings on the left navigation menu of the **Logs** tab. The event and data logs display no button to clear the log.
  - In the command line interface, the equivalent features and options.

  The default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same tabs and menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. The event and data logs display no button to clear the log.

  The default user name is **readonly**, and the default password is **apc**. To set **User Name** and **Password** values for the three account types above, see “Setting user access” on page 55.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Rack PDU uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

The Rack PDU implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Rack PDU does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

Resetting the network timer

To ensure that the Rack PDU does not restart if the network is quiet for 9.5 minutes, the Rack PDU attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the Rack PDU, and the response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the subnet. The network traffic of that computer will restart the 9.5-minute time frequently enough to prevent the Rack PDU from restarting.

Network Port Sharing

About the Network Port Sharing Feature

You can use the Network Port Sharing feature to view the status of and configure and manage up to four Rack PDUs using only one network connection. This is made possible by connecting the Rack PDUs via the "In" and "Out" ports on the Rack PDU front panel.
Note: All Rack PDUs in the group must be using the same Rack PDU firmware revision, 5.1.5 or later (excluding v6.0.5 EnergyWise), in order to support the Network Port Sharing Feature.

Display ID

The display ID is a number, 1 to 4, used to uniquely identify the Rack PDUs in a group. After two or more Rack PDUs are connected to one another in a group, they can be identified on the various interfaces by the use of this "Display ID". This Display ID is viewable on the LCD by selecting the Display Settings > Display ID > Show option on the LCD keypad.

Installation Instructions

Connect up to four Rack PDUs. Insert an RJ45 terminator (included) in the unused "In"/"Out" ports on each end of the chain.

Note: Failure to use terminators may cause a loss of communication on the Rack PDUs.
Note: To reduce the possibility of communication issues, the maximum total length of cabling connecting Rack PDUs in a group should not exceed 10 meters. All Rack PDUs in a Network Port Sharing group should reside in the same rack enclosure.

Connect the "Network" port of one of the grouped Rack PDUs to a network hub or switch. This unit will be the "Host" for the Rack PDU group. A Host is defined as a Rack PDU that is connected to the network and is part of a Rack PDU group. Set up network functionality for this Host Rack PDU as specified in the Establish Network Settings section. The Host will automatically discover any "Guest" PDUs connected via In/Out ports. The Rack PDU group is now available via the Host's IP address.

Specific assignment of Display IDs. Follow the instructions below before powering up any of the Rack PDUs in the group.

If it is desired to have a specific assignment of Display IDs, this can be achieved by powering up the units for the first time in the desired order, 1 to 4. For example, before powering up any of the Rack PDUs connected in a group, determine the Display ID order that you would like. Then, first power up the unit that you would like to have Display ID 1. After that unit has initialized and the LCD has started displaying its screens, power on the unit that you would like to have Display ID 2. Continue in the same way for units 3 and 4, if applicable for your setup.

Note: The Display ID can be configured from the web interface via the "Device Manager > Load Management > device load > Display ID" field.

Getting Started

To start using the Rack PDU:

1. Install the Rack PDU using the *Rack Power Distribution Unit Installation Instructions* that were shipped with your Rack PDU.
2. Apply power and connect to your network. Follow the directions in the *Rack Power Distribution Unit Installation Instructions*.
3. Establish network settings. (See “Establish Network Settings” on page 5.)
4. Begin using the Rack PDU by way of one of the following:
   - “Web Interface” on page 40
   - “Command Line Interface” on page 14
   - “Rack PDU Front Panel” on page 9

Establish Network Settings

Note: Disregard the procedures described in this section if you have StruxureWare Data Center Expert as part of your system. See the documentation for your StruxureWare Data Center Expert device for more information.

You must configure the following TCP/IP settings before the Rack PDU can operate on a network:

- IP address of the Rack PDU
- Subnet mask
- Default gateway

  Note: If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the Rack PDU and that is usually running. The Rack PDU uses the default gateway to test the network when traffic is very light.

  Note: Do not use the loopback address (127.0.0.1) as the default gateway address for the Rack PDU. It disables the card and requires you to reset TCP/IP settings to their defaults using a local serial login.

  See “Watchdog Features” on page 3 for more information about the watchdog role of the default gateway.

TCP/IP configuration methods

Use one of the following methods to define the TCP/IP settings needed by the Rack PDU:

- “Device IP Configuration Wizard” on page 80
- “DHCP and BOOTP configuration” on page 5
- “Command Line Interface” on page 7

INI file utility

You can use the INI file export utility to export INI file settings from configured Rack PDUs to one or more unconfigured Rack PDUs. For more information, see “Use an .ini File” on page 77.

DHCP and BOOTP configuration

The default TCP/IP configuration setting, **DHCP**, assumes that a properly configured DHCP server is available to provide TCP/IP settings to Rack PDU. You can also configure the setting for BOOTP.

A user configuration (INI) file can function as a BOOTP or DHCP boot file. For more information, see “Use an .ini File” on page 77.

If neither of these servers is available, see “Device IP Configuration Wizard” on page 80 or “Command Line Interface” on page 7.

BOOTP. For the Rack PDU to use a BOOTP server to configure its TCP/IP settings, it must find a properly configured RFC951-compliant BOOTP server.

In the BOOTPTAB file of the BOOTP server, enter the Rack PDU’s MAC address, IP address, subnet mask, and default gateway, and, optionally, a bootup file name. Look for the MAC address on the bottom of the Rack PDU or on the Quality Assurance slip included in the package.

When the Rack PDU reboots, the BOOTP server provides it with the TCP/IP settings.

- If you specified a bootup file name, the Rack PDU attempts to transfer that file from the BOOTP server using TFTP or FTP. The Rack PDU assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Rack PDU remotely through its “Web Interface” on page 40 or “Command Line Interface” on page 7; the user name and password are both **apc**, by default. To create a bootup file, see your BOOTP server documentation.

DHCP. You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Rack PDU.

This section summarizes the Rack PDU’s communication with a DHCP server. For more detail about how a DHCP server can configure the network settings for a Rack PDU, see “DHCP response options” on page 60.

1. The Rack PDU sends out a DHCP request that uses the following to identify itself:
   – A Vendor Class Identifier (APC by default)
   – A Client Identifier (by default, the MAC address of the Rack PDU)
   – A User Class Identifier (by default, the identification of the application firmware installed on the Rack PDU)
   – A Host Name (by default, apcXXYYZZ with XXYYZZ being the last six digits of the PDU). This is known as DHCP Option 12.
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the Rack PDU needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Rack PDU can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The Rack PDU does not require this cookie by default.)

   ```
   Option 43 = 01 04 31 41 50 43
   ```

   Where:
   – The first byte (`01`) is the code.
   – The second byte (`04`) is the length.
   – The remaining bytes (`31 41 50 43`) are the APC cookie.
   See your DHCP server documentation to add code to the Vendor Specific Information option.

   Note: By selecting the **Require vendor specific cookie to accept DHCP Address** check box in the Web interface, you can require the DHCP server to provide an “APC” cookie, which supplies information to the Rack PDU: **Administration > Network**>**TCP/IP**>**ipv4 settings**.

Command Line Interface

1. Log on to the command line interface. See “Log on to the Command Line Interface” on page 14.
2. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack PDU.
3. Use these three commands to configure network settings. (Text in italics indicates a variable.)
   a. `tcpip -i yourIPaddress`
   b. `tcpip -s` *`yourSubnetMask`*
   c. `tcpip -g` *`yourDefaultGateway`*

   For each variable, type a numeric value that has the format *`xxx.xxx.xxx.xxx`*.

   For example, to set a system IP address of 156.205.14.141, type the following command and press ENTER:
   `tcpip -i 156.205.14.141`
4. Type `exit`. The Rack PDU restarts to apply the changes.

Recovering from a Lost Password

You can use a local computer (a computer that connects to the Rack PDU or other device through the serial port) to access the command line interface.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable (APC part number 940-0144A) to the selected port on the computer and to the Serial port at the Rack PDU.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   – The serial port is not in use by another application.
   – The terminal settings are correct as specified in step 3.
   – The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER, repeatedly if necessary, to display the **User Name** prompt again, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is re-displayed, you must repeat step 5 and log on again.)
7. At the command line interface, use the following commands to change the **User Name** and **Password** settings, both of which are now **apc**:

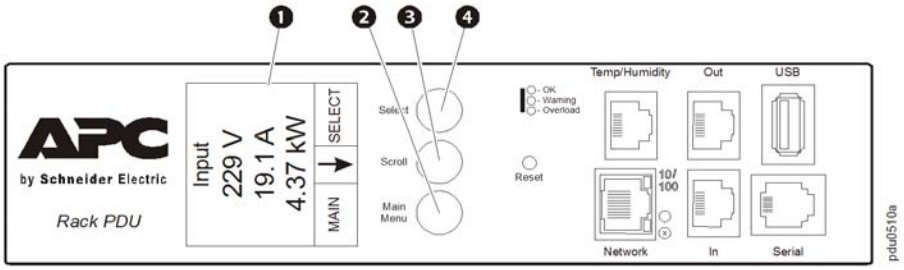
   ```
   user -an yourAdministratorName
   user -ap yourAdministratorPassword
   ```

   For example, to change the Administrator user name to **Admin**, type:

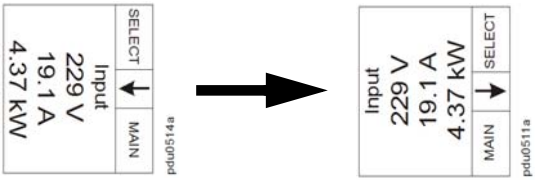
   ```
   user -an Admin
   ```

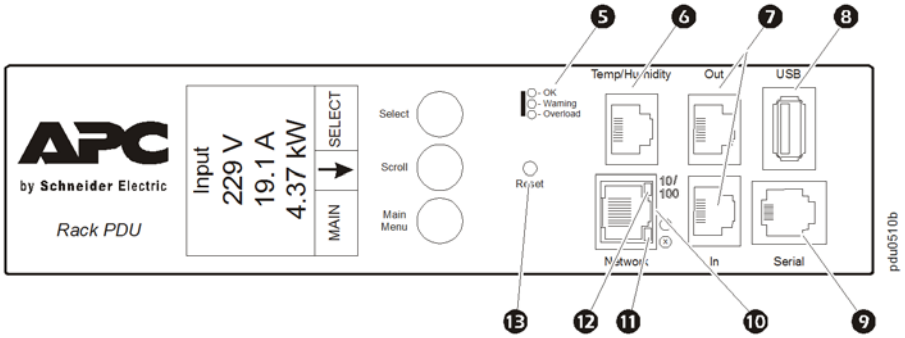
8. Type quit or exit to log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Rack PDU Front Panel



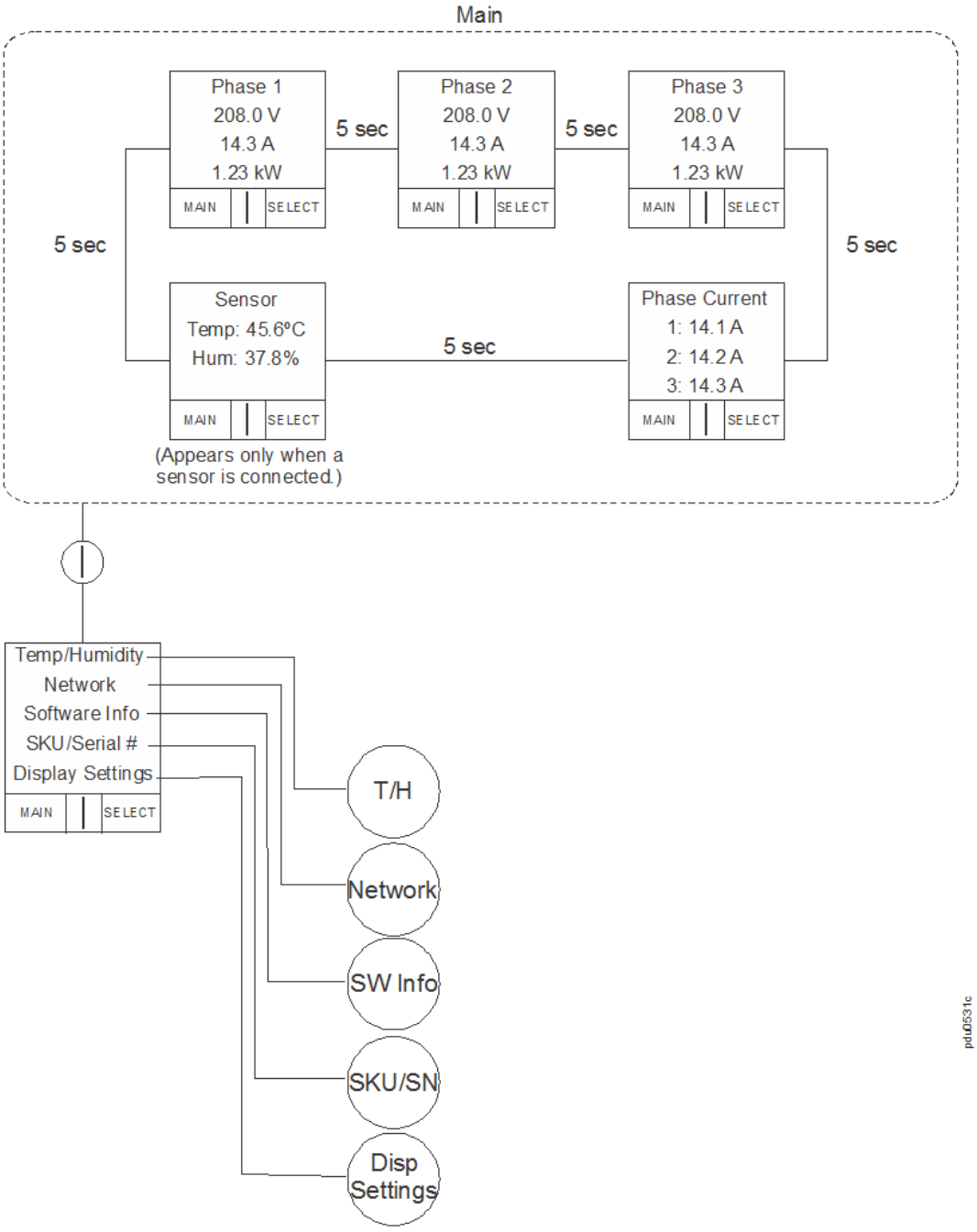
Note: Your APC product is configured so the display backlight turns off after 10 minutes of inactivity. The backlight can be turned on by depressing any button below the display.

Item		Function
❶	Display	Shows information about the Rack PDU. In normal operation, input voltage, current, and power refreshes every five seconds. To reverse the text, press and hold simultaneously for five seconds the Main Menu (❷), Scroll (❸), and Select (❹) buttons. 
❷	Main Menu button	Press to view the Rack PDU electrical input, shown below.
❸	Scroll button	Press once to display the menu. Press additional times to highlight the desired menu option.
❹	Select button	With a menu option highlighted, press the Select button to display Rack PDU information. Software Info is shown below.



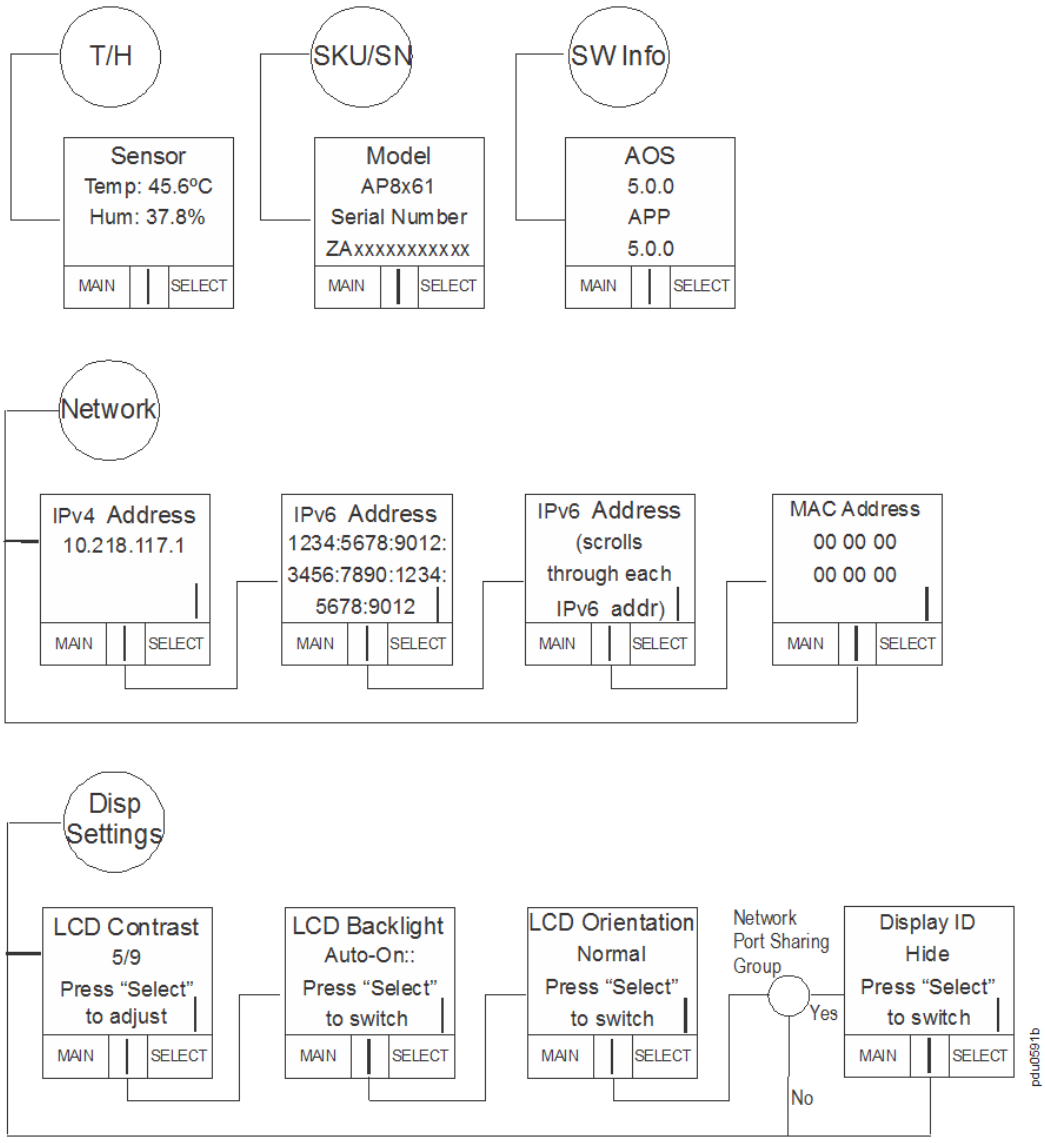
Item		Function
❺	OK, Warning, Overload LED	Indicates the status of the Rack PDU load. See “Load indicator LED” on page 13.
❻	Temp/Humidity port	Port for connecting an APC Temperature Sensor (AP9335T) or an APC Temperature/Humidity Sensor (AP9335TH).
❼	In and Out ports	For use with the Network Port Sharing feature.
❽	USB port	(For use with a flash drive for firmware upgrades - 5V @ 100ma.)
❾	RJ-12 Serial Port	Port for connecting the Rack PDU to a terminal emulator program for local access to the command line interface. Use the supplied serial cable (APC part number 940-0144A).
❿	10/100 Base-T Connector	Connects the Rack PDU to the network.
⓫	Network status LED	See “Network Status LED” on page 13.
⓬	10/100 LED	See “10/100 LED” on page 13.
⓭	Reset button	Resets the Rack PDU without affecting the outlet status.

Display Tree Example 1



Display Tree Example 2

Note: "Temp/Humidity" only appears when an AP9335T or AP9335TH sensor is attached.



Network Status LED

Condition	Description
Off	One of the following situations exists: • The Rack PDU is not receiving input power. • The Rack PDU is not operating properly. It may need to be repaired or replaced. Contact APC Customer Support.
Solid Green	The Rack PDU has valid TCP/IP settings.
Solid Orange	A hardware failure has been detected in the Rack PDU. Contact APC Customer Support.
Flashing Green	The Rack PDU does not have valid TCP/IP settings.
Flashing Orange	The Rack PDU is making BOOTP requests.
Alternately flashing green and orange	If the LED is flashing slowly, the Rack PDU is making DHCP[2] requests[1]. If the LED is flashing rapidly, the Rack PDU is starting up.
1. If you do not use a BOOTP or DHCP server, see “Establish Network Settings” on page 5 to configure the TCP/IP settings of the Rack PDU. 2. To use a DHCP server, see “TCP/IP and Communication Settings” on page 59.	

10/100 LED

Condition	Description
Off	One or more of the following situations exists: • The Rack PDU is not receiving input power. • The cable that connects the Rack PDU to the network is disconnected or defective • The device that connects the Rack PDU to the network is turned off. • The Rack PDU itself is not operating properly. It may need to be repaired or replaced. Contact APC Customer Support.
Solid green	The Rack PDU is connected to a network operating at 10 Megabits per second (Mbps).
Solid orange	The Rack PDU is connected to a network operating at 100 Mbps.
Flashing green	The Rack PDU is receiving or transmitting data packets at 10 Mbps.
Flashing orange	The Rack PDU is receiving or transmitting data packets at 100 Mbps.

Load indicator LED

The load indicator LED identifies overload and warning conditions for the Rack PDU.

Condition	Description
Solid Green	OK. No load alarms (warning or critical) are present.
Solid Yellow	Warning. At least one load warning alarm is present, but no critical alarms are present.
Flashing Red	Overload. At least one load critical alarm is present.

Command Line Interface

About the Command Line Interface

You can use the command line interface to view the status of and configure and manage the Rack PDU. In addition, the command line interface enables you to create scripts for automated operation. An Administrator has full access to the command line interface, a Device user has limited access, and a Read-Only user is completely restricted. (For additional details, see “Types of User Accounts” on page 2.)

You can configure all parameters of a Rack PDU (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the Rack PDU. The CLI uses XMODEM to perform the transfer. However, you cannot read the current INI file through XMODEM.

Log on to the Command Line Interface

To access the command line interface, you can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network as the Rack PDU.

Remote access to the command line interface

You can access the command line interface through Telnet or SSH. Telnet is enabled by default. Enabling SSH disables Telnet.

To enable or disable these access methods, use the Web interface. On the **Administration** tab, select **Network** on the top menu bar, and then the **access** option under **Console** on the left navigation menu.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

To use Telnet to access the command line interface:

1. From a computer that has access to network on which the Rack PDU is installed, at a command prompt, type `telnet` and the IP address for the Rack PDU (for example, `telnet 139.225.6.133`, when the Rack PDU uses the default Telnet port of 23), and press ENTER.

   If the Rack PDU uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general usage: some clients don’t allow you to specify the port as an argument and some types of Linux might want extra commands).

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User).

   If you cannot remember your user name or password, see “Recovering from a Lost Password” on page 8.

SSH for high-security access. If you use the high security of SSL for the Web interface, use SSH for access to the command line interface. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Local access to the command line interface

For local access, use a computer that connects to the Rack PDU through the serial port to access the command line interface:

1. Select a serial port at the computer and disable any service that uses that port.
2. Connect the serial cable (APC part number 940-0144A) from the selected serial port on the computer to the **Serial** port on the Rack PDU.
3. Run a terminal program (e.g., HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER. At the prompts, enter your user name and password.

About the Main Screen

Following is an example of the main screen, which is displayed when you log on to the command line interface of a Rack PDU.

```
American Power Conversion              Network Management Card AOS  vx.x.x
(c)Copyright 2012 All Rights Reserved  RPDU 2g                      vx.x.x
-------------------------------------------------------------------------
Name     : Test Lab                                  Date : 10/30/2012
Contact  : Don Adams                                 Time : 5:58:30
Location : Building 3                                User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N4+ N6+ A+

APC>
```

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. In the example above, the application firmware for the Rack PDU is displayed.

  ```
  Network Management Card AOS   vx.x.x
  RPDU 2g                       vx.x.x
  ```

- Three fields identify the system name, contact person, and location of the Rack PDU.

  ```
  Name     : Test Lab
  Contact  : Don Adams
  Location : Building 3
  ```

- An **Up Time** field reports how long the Rack PDU has been running since it was last turned on or reset.

  ```
  Up Time  : 0 Days, 21 Hours, 21 Minutes
  ```

- Two fields identify when you logged in, by date and time.

  ```
  Date : 10/30/2012
  Time : 5:58:30
  ```

- The **User** field identifies whether you logged in through the **Administrator** or **Device Manager** account. (The **Read Only User** account cannot access the command line interface.)

  ```
  User : Administrator
  ```

- A **Stat** field reports the Rack PDU status.

  ```
  Stat : P+ N4 N6
  ```

P+	The APC operating system (AOS) is functioning properly.

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N+	N4+ N6+	The network is functioning properly.
N?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N–	N6-	N4- N6-	The Rack PDU failed to connect to the network.
N!	N6!	N4! N6!	Another device is using the Rack PDU IP address.
* The N4 and N6 values can be different from one another: you could, for example, have N4- N6+.			

A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

Note: If P+ is not displayed, contact APC support staff.

Using the Command Line Interface

At the command line interface, use commands to configure the Rack PDU. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the command line interface, you can also do the following:

- Type `?` and press ENTER to view a list of available commands, based on your account type.
- To obtain information about the purpose and syntax of a specified command, type the command, a space, and `?` or the word `help`. For example, to view RADIUS configuration options, type:

  ```
  radius ?
  ```

  or

  ```
  radius help
  ```

- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text you typed in the command line.
- Type `exit` or `quit` to close the connection to the command line interface.

Command Syntax

Item	Description
-	Options are preceded by a hyphen.
< >	Definitions of options are enclosed in angle brackets. For example: `-dp <device password>`
[ ]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
|	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.

Example of a command that supports multiple options:

```
user [-an <admin name>] [-ap <admin password>]
```

In this example, the user command accepts the option `-an`, which defines the Administrator user name, and the option `-ap`, which defines the Administrator password. To change the Administrator user name and password to XYZ:

1. Type the user command, one option, and the argument `XYZ`:
   `user -ap XYZ`
2. After the first command succeeds, type the user command, the second option, and the argument `XYZ`:
   `user -an XYZ`

Example of a command that accepts mutually exclusive arguments for an option:

```
alarmcount -p [all | warning | critical]
```

In this example, the option -p accepts only three arguments: all, warning, or critical. For example, to view the number of active critical alarms, type:
`alarmcount -p critical`

The command will fail if you type an argument that is not specified.

Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text:

The CLI reports all command operations with the following format:

```
E [0-9] [0-9] [0-9] : Error message
```

Code	Message
E000	Success
E001	Successfully Issued
E002	Reboot required for change to take effect
E100	Command failed
E101	Command not found
E102	Parameter Error
E103	Command Line Error
E104	User Level Denial
E105	Command Prefill
E106	Data Not Available
E107	Serial communication with the Rack PDU has been lost

Network Management Card Command Descriptions

Access: Administrator, Device User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by a question mark.

Example: To view a list of options that are accepted by the `alarmcount` command, type:

```
alarmcount ?
```

about

Access: Administrator, Device User

Description: View hardware and firmware information. This information is useful in troubleshooting and enables you to determine if updated firmware is available at the APC Web site.

alarmcount

Access: Administrator, Device User

Description:

Option	Arguments	Description
-p	all	View the number of active alarms reported by the Rack PDU. Information about the alarms is provided in the event log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.

Example: To view all active warning alarms, type:

```
alarmcount -p warning
```

boot

Access: Administrator only

Description: Define how the Rack PDU will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the Rack PDU turns on, resets, or restarts. See “TCP/IP and Communication Settings” on page 59 for information about each boot mode setting.
-c	enable | disable	`dhcp` and `dhcpBootp` boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
The default values for these three settings generally do not need to be changed: -v <vendor class>: APC -i <client id>: The MAC address of the Rack PDU, which uniquely identifies it on the network -u <user class>: The name of the application firmware module		

Example: To use a DHCP server to obtain network settings:

1. Type `boot -b dhcp`
2. Enable the requirement that the DHCP server provide the APC cookie:
   `boot -c enable`

cd

Access: Administrator, Device User

Description: Navigate to a folder in the directory structure of the Rack PDU.

Example 1: To change to the `ssh` folder and confirm that an SSH security certificate was uploaded to the Rack PDU:

1. Type `cd ssh` and press ENTER.
2. Type `dir` and press ENTER to list the files stored in the SSH folder.

Example 2: To return to the main directory folder, type:

```
cd ..
```

clrrst

Access: Administrator, Device User

Description: Clear reset reason.

console

Access: Administrator only

Description: Define whether users can access the command line interface using Telnet, which is enabled by default, or Secure SHell (SSH), which provides protection by transmitting user names, passwords, and data in encrypted form. You can change the Telnet or SSH port setting for additional security. Alternately, disable network access to the command line interface.

Option	Argument	Description
-S	disable | telnet | ssh	Configure access to the command line interface, or use the `disable` command to prevent access. Enabling SSH enables SCP and disables Telnet.
-pt	<telnet port n>	Define the Telnet port used to communicate with the Rack PDU (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the Rack PDU (22 by default).
-b	2400 | 9600 | 19200 | 38400	Configure the speed of the serial port connection (9600 bps by default).

Example 1: To enable SSH access to the command line interface, type:
```
console -S ssh
```

Example 2: To change the Telnet port to 5000, type:
```
console -pt 5000
```

date

Access: Administrator only

Definition: Configure the date used by the Rack PDU.

To configure an NTP server to define the date and time for the Rack PDU, see “Set the Date and Time” on page 76.

Option	Argument	Description
-d	<“datestring”>	Set the current date. Use the date format specified by the `date -f` command.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.
-z	<time zone offset>	Set the difference with GMT in order to specify your time zone. This enables you to synchronize with other people in different time zones.

Example 1: To display the date using the format yyyy-mm-dd, type:
`date -f yyyy-mm-dd`

Example 2: To define the date as October 30, 2009, using the format configured in the preceding example, type:
`date -d “2009-10-30”`

Example 3: To define the time as 5:21:03 p.m., type:
`date -t 17:21:03`

delete

Access: Administrator only

Description: Delete a file in the file system.

Argument	Description
<file name>	Type the name of the file to delete.

dir

Access: Administrator, Device User

Description: View the files and folders stored on the Rack PDU.

dns

Access: Administrator only

Definition: Configure the manual Domain Name System (DNS) settings.

Parameter	Argument	Description
-OM	enable | disable	Override the manual DNS.
-p	<primary DNS server>	Set the primary DNS server.
-s	<secondary DNS server>	Set the secondary DNS server.
-d	<domain name>	Set the domain name.
-n	<domain name IPv6>	Set the domain name IPv6.
-h	<host name>	Set the host name.

eventlog

Access: Administrator, Device User

Description: View the date and time you retrieved the event log, the status of the Rack PDU, and the status of sensors connected to the Rack PDU. View the most recent device events and the date and time they occurred. Use the following keys to navigate the event log:

Key	Description
ESC	Close the event log and return to the command line interface.
ENTER	Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log.
SPACEBAR	View the next page of the event log.
B	View the preceding page of the event log. This command is not available at the main page of the event log.
D	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

exit

Access: Administrator, Device User

Description: Exit from the command line interface session.

format

Access: Administrator only

Description: Reformat the file system of the Rack PDU and erase all security certificates, encryption keys, configuration settings, and the event and data logs. Be careful with this command.
Note: To reset the Rack PDU to its default configuration, use the `resetToDef` command.

FTP

Access: Administrator only

Description: Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port from 5001 to 32768 for added security.

Option	Argument	Definition
-p	<port number>	Define the TCP/IP port that the FTP server uses to communicate with the Rack PDU (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-S	enable | disable	Configure access to the FTP server.

Example: To change the TCP/IP port to 5001, type:
`ftp -p 5001`

help

Access: Administrator, Device User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by `help`.

Example 1: To view a list of commands available to someone logged on as a Device User, type:
`help`

Example 2: To view a list of options that are accepted by the `alarmcount` command, type:
`alarmcount help`

netstat

Access: Administrator, Device User

Description: View the status of the network and all active IPv4 and IPv6 addresses.

ntp

Access: Administrator

Description: View and configure the network time protocol parameters.

Option	Argument	Definition
-OM	enable | disable	Override the manual settings.
-p	<primary NTP server>	Specify the primary server.
-s	<secondary NTP server>	Specify the secondary server.

Example 1: To enable the override of manual setting, type:
`ntp -OM enable`

Example 2: To specify the primary NTP server, type:
`ntp -p 150.250.6.10`

ping

Access: Administrator, Device User

Description. Determine whether the device with the IP address or DNS name you specify is connected to the network. Four inquiries are sent to the address.

Argument	Description
<IP address or DNS name>	Type an IP address with the format *xxx.xxx.xxx.xxx*, or the DNS name configured by the DNS server.

Example: To determine whether a device with an IP address of 150.250.6.10 is connected to the network, type:
`ping 150.250.6.10`

portSpeed

Access: Administrator

Description:

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100 F	Define the communication speed of the Ethernet port. The `auto` command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 61 for more information about the port speed settings.

Example: To configure the TCP/IP port to communicate using 100 Mbps with half-duplex communication (communication in only one direction at a time), type:
`portspeed -s 100H`

prompt

Access: Administrator, Device User

Description: Configure the command line interface prompt to include or exclude the account type of the currently logged-in user. Any user can change this setting; all user accounts will be updated to use the new setting.

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: `APC>`

Example: To include the account type of the currently logged-in user in the command prompt, type:
`prompt -s long`

quit

Access: Administrator, Device User

Description: Exit from the command line interface session (this works the same as the exit command).

radius

Access: Administrator only

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Configure the RADIUS Server” on page 57.
Additional authentication parameters for RADIUS servers are available at the Web interface of the Rack PDU. See “RADIUS” on page 56 for more information.
For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at **www.apc.com**.

Option	Argument	Description
-a	local | radiusLocal | radius	Configure RADIUS authentication: `local`—RADIUS is disabled. Local authentication is enabled. `radiusLocal`—RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. `radius`—RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary RADIUS server. **Note:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the Rack PDU.
-t1 -t2	<server timeout>	The time in seconds that the Rack PDU waits for a response from the primary or secondary RADIUS server.

Example 1:
To view the existing RADIUS settings for the Rack PDU, type `radius` and press ENTER.

Example 2: To enable RADIUS and local authentication, type:
```
radius -a radiusLocal
```

Example 3: To configure a 10-second timeout for a secondary RADIUS server, type:
```
radius -t2 10
```

reboot

Access: Administrator only

Description: Restart the interface of the Rack PDU.

resetToDef

Access: Administrator only

Description: Reset all parameters to their default.

Option	Arguments	Description
-p	all | keepip	Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

Example: To reset all of the configuration changes *except* the TCP/IP settings for the Rack PDU, type:
`resetToDef -p keepip`

snmp, snmpv3

Access: Administrator only

Description: Enable or disable SNMP 1 or SNMP 3.

Option	Arguments	Description
-S	enable | disable	Enable or display the respective version of SNMP, 1 or 3.

Example: To enable SNMP version 1, type:
`snmp -S enable`

system

Access: Administrator only

Description: View and set the system name, the contact, the location and view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A (see “About the Main Screen” on page 15 for more information about system status).

Option	Argument	Description
-n	<system name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. **Note:** If you define a value with more than one word, you must enclose the value in quotation marks. These values are also used by StruxureWare Data Center Expert and the Rack PDU’s SNMP agent.
-c	<system contact>	
-l	<system location>	

Example 1: To set the device location as `Test Lab`, type:
`system -l “Test Lab”`

Example 2: To set the system name as `Don Adams`, type:
`system -n “Don Adams”`

tcpip

Access: Administrator only

Description: View and manually configure these network settings for the Rack PDU:

Option	Argument	Description
-i	<IP address>	Type the IP address of the Rack PDU, using the format *xxx.xxx.xxx.xxx*
-s	<subnet mask>	Type the subnet mask for the Rack PDU.
-g	<gateway>	Type the IP address of the default gateway. **Do not** use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the Rack PDU will use.

Example 1: To view the network settings of the Rack PDU, type `tcpip` and press ENTER.

Example 2: To manually configure an IP address of `150.250.6.10` for the Rack PDU, type:
`tcpip -i 150.250.6.10`

tcpip6

Access: Administrator only

Description: Enable IPv6 and view and manually configure these network settings for the Rack PDU:

Option	Argument	Description
-S	enable | disable	Enable or disable IPv6.
-man	enable | disable	Enable manual addressing for the IPv6 address of the Rack PDU.
-auto	enable | disable	Enable the Rack PDU to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the Rack PDU.
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway.
-d6	router | statefull | statelss | never	Set the DHCPv6 mode, with parameters of router controlled, statefull (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), never.

Example 1: To view the network settings of the Rack PDU, type `tcpip6` and press ENTER.

Example 2: To manually configure an IPv6 address of `2001:0:0:0:0:FFD3:0:57ab for the` Rack PDU, type:
`tcpip6 -i 2001:0:0:0:0:FFD3:0:57ab`

user

Access: Administrator only

Description: Configure the user name, password, and inactivity timeout for the Administrator, Device User, and Read-Only User account types. For information on the permissions granted to each account type, see “Types of User Accounts” on page 2.

Option	Argument	Description
-an -dn -rn	<admin name> <device name> <read-only name>	Set the case-sensitive user name for each account type. The maximum length is 10 characters.
-ap -dp -rp	<admin password> <device password> <read-only password>	Set the case-sensitive password for each account type. The maximum length is 32 characters. Blank passwords (passwords with no characters) are not allowed.
-t	<minutes>	Configure the time (3 minutes by default) that the system waits before logging off an inactive user.

Example 1: To change the Administrator user name to XYZ, type:
```
user -an XYZ
```

Example 2: To change the log off time to 10 minutes, type:
```
user -t 10
```

web

Access: Administrator only

Description: Enable access to the Web interface using HTTP or HTTPS.

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 to 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114, type:
```
http://152.214.12.114:5000
```

Option	Argument	Definition
-S	disable | http | https	Configure access to the Web interface. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-ph	<http port #>	Define the TCP/IP port used by HTTP to communicate with the Rack PDU (80 by default).
-ps	<https port #>	Define the TCP/IP port used by HTTPS to communicate with the Rack PDU (443 by default).

Example: To prevent all access to the Web interface, type:
```
web -S disable
```

xferINI

Access: Administrator only

Description: Use XMODEM to upload an INI file while you are accessing the command line interface through a serial connection. After the upload completes:

- If there are any system or network changes, the command line interface restarts and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the Rack PDU, you must reset the baud rate to the default to reestablish communication with the Rack PDU.

xferStatus

Access: Administrator only

Description: View the result of the last file transfer. See “Verifying Upgrades and Updates” on page 91 for descriptions of the transfer result codes.

Device Command Descriptions

Network Port Sharing Commands

The Command Line Interface allows commands to be sent to guest Rack PDUs. The user may specify the Display ID of the Rack PDU to be commanded, followed by a colon, before the first argument (or as the first argument, if the command does not normally have arguments). Providing a Display ID is optional, omitting it will simply command the local Rack PDU. For example:

<command> <id>:<arg1> <arg2>

This will send <command> to the Rack PDU with the Display ID <id>. <id> is delimited from <arg1> with a colon character; do not include any spaces between <id>:<arg1>, as spaces are used to delimit arguments.

bkLowLoad

Access: Administrator, Device User

Description: Set or view the bank low-load threshold current in amps. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Example 1: To set the low-load threshold for all banks to 1A, type:

```
apc> bkLowLoad all 1
E000: Success
```

Example 2: To view the low-load threshold setting for banks 1 through 3, type:

```
apc> bkLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

Example 3: To view the low-load threshold setting for banks 1 and 2 on guest Rack PDU 3, type:

```
apc> bkLowLoad 3:1-2
E000: Success
1: 0 A
2: 0 A
```

bkNearOver

Access: Administrator, Device User

Description: Set or view the bank near-overload threshold current in amps. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Example 1: To set the near-overload threshold for all banks to 10A, type:

```
apc> bkNearOver all 10
E000: Success
```

Example 2: To view the near-overload threshold setting for banks 1 through 3, type:

```
apc> bkNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

bkOverLoad

Access: Administrator, Device User

Description: Set or view the bank overload threshold current in amps. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Example 1: To set the bank overload threshold for all banks to 13A, type:

```
apc> bkOverLoad all 13
E000: Success
```

Example 2: To view the bank overload threshold setting for banks 1 through 3, type:

```
apc> bkOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

bkReading

Access: Administrator, Device User

Description: View the current reading (measurement) in amps for a bank. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Example 1: To view the current reading for bank 3, type:

```
apc> bkReading 3
E000: Success
3: 4.2 A
```

Example 2: To view the current reading for all banks, type:

```
apc> bkReading all
E000: Success
1: 6.3 A
2: 5.1 A
3: 4.2 A
```

devLowLoad

Access: Administrator, Device User

Description: Set or view the low-load threshold in kilowatts for the device.

Example 1: To view the low-load threshold, type:

```
apc> devLowLoad
E000: Success
0.5 kW
```

Example 2: To set the low-load threshold to 1 kW, type:

```
apc> devLowLoad 1.0
E000: Success
```

Example 3: To set the low-load threshold to 1.5 kW on guest Rack PDU 3, type:

```
apc> devLowLoad 3:1.5
E000: Success
```

devNearOver

Access: Administrator, Device User

Description: Set or view the near-overload threshold in kilowatts for the device.

Example 1: To view the near-overload threshold, type:

```
apc> devNearOver
E000: Success
20.5 kW
```

Example 2: To set the near-overload threshold to 21.3 kW, type:

```
apc> devNearOver 21.3
E000: Success
```

devOverLoad

Access: Administrator, Device User

Description: Set or view the overload threshold in kilowatts for the device.

Example 1: To view the overload threshold, type:

```
apc> devOverLoad
E000: Success
25.0 kW
```

Example 2: To set the overload threshold to 25.5 kW, type:

```
apc> devOverLoad 25.5
E000: Success
```

Example 3: To view the overload threshold for guest Rack PDU 3, type:

```
apc> devOverLoad 3:
E000: Success
5.0 kW
```

devReading

Access: Administrator, Device User

Description: View the total power in kilowatts or total energy in kilowatt-hours for the device.

Argument	Definition
power	View the total power in kilowatts.
energy	View the total energy in kilowatt-hours.

Example 1: To view the total power, type:

```
apc> devReading power
E000: Success
5.2 kW
```

Example 2: To view the total energy, type:

```
apc> devReading energy
E000: Success
200.1 kWh
```

Example 3: To view the total power for guest Rack PDU 3, type:

```
apc> devReading 3:power
E000: Success
4.2 kW
```

humLow

Access: Administrator, Device User

Description: Set or view the low humidity threshold as a percent of the relative humidity.

Example 1: To view the low humidity threshold, type:

```
apc> humLow
E000: Success
10 %RH
```

Example 2: To set the low humidity threshold, type:

```
apc> humLow 12
E000: Success
```

Example 3: To view the low humidity threshold on guest Rack PDU 3, type:

```
apc> humLow 3:
E000: Success
10 %RH
```

humMin

Access: Administrator, Device User

Description: Set or view the minimum humidity threshold as a percent of the relative humidity.

Example 1: To view the minimum humidity threshold, type:

```
apc> humMin
E000: Success
6 %RH
```

Example 2: To set the minimum humidity threshold, type:

```
apc> humMin 8
E000: Succes
```

Example 3: To set the minimum humidity threshold on guest Rack PDU 3 to 18% RH, type:

```
apc> humMin 3:18
E000: Success
```

humReading

Access: Administrator, Device User

Description: View the humidity value from the sensor.

Example 1: To view the humidity value, type:

```
apc> humReading
E000: Success
25 %RH
```

Example 2: To view the humidity value on guest Rack PDU 2, type:

```
apc> humReading 2:
E000: Success
48 %RH
```

phLowLoad

Access: Administrator, Device User

Description: Set or view the phase low-load threshold in kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To set the low-load threshold for all phases to 1 kW, type:

```
apc> phLowLoad all 1
E000: Success
```

Example 2: To view the low-load threshold for phases 1 through 3, type:

```
apc> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

Example 3: To view the low-load threshold for phases 1 on guest Rack PDU 3, type:

```
apc> phLowLoad 3:1
E000: Success
1: 1 A
```

phNearOver

Access: Administrator, Device User

Description: Set or view the phase near-overload threshold in kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To set the near-overload threshold for all phases to 10 kW, type:

```
apc> phNearOver all 10
E000: Success
```

Example 2: To view the near-overload threshold for phases 1 through 3, type:

```
apc> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

phOverLoad

Access: Administrator, Device User

Description: Set or view the phase overload threshold in kilowatts. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Example 1: To set the overload threshold for all phases to 13 kW, type:

```
apc> phOverLoad all 13
E000: Success
```

Example 2: To view the overload threshold for phases 1 through 3, type:

```
apc> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

phReading

Access: Administrator, Device User

Description: View the current, voltage, or power for a phase. Set or view the phase near-overload threshold in kilowatts. You can specify all phases, a single phase, a range, or a comma-separated list of phases.

Example 1: To view the measurement for current for phase 3, type:

```
apc> phReading 3 current
E000: Success
3: 4 A
```

Example 2: To view the voltage for each phase, type:

```
apc> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

Example 3: To view the power for phase 2 on guest Rack PDU 3, type:

```
apc> phReading 3:2 power
E000: Success
2: 40 W
```

prodInfo

Access: Administrator, Device User

Description: View information about the Rack PDU.

Example 1: To view the product information for this Rack PDU, type:

```
apc> prodInfo
E000: Success
AOS X.X.X
Metered Rack PDU X.X.X
Model:            AP8XXX
Present Outlets:  XX
Switched Outlets: XX
Metered Outlets:  XX
Max Current:      XX A
Phases:           X
Banks:            X
```

Example 2: To view the product information for guest Rack PDU 2, type::

```
apc> prodInfo 2:
E000: Success
AOS X.X.X
Metered Rack PDU X.X.X
Model:            AP8XXX
Present Outlets:  XX
Switched Outlets: XX
Metered Outlets:  XX
Max Current:      XX A
Phases:           X
Banks:            X
```

sensorName

Access: Administrator, Device User

Description: Set or view the name assigned to the Rack PDU Temp/Humidity port.

Example 1: To set the name for the port to “Sensor1,” type:

```
apc> sensorName Sensor1
E000: Success
```

Example 2: To then view the name for the sensor port, type:

```
apc> sensorName
E000: Success
Sensor1
```

Example 3: To set the name for the sensor port on guest Rack PDU 2 to “Sensor1,” type:

```
apc> sensorName 2:Sensor1
E000: Success
```

tempHigh

Access: Administrator, Device User

Description: Set or view the high-temperature threshold in either Fahrenheit or Celsius.

Example 1: To set the high-temperature threshold to 70º Fahrenheit, type:

```
apc> tempHigh F 70
E000: Success
```

Example 2: To view the high-temperature threshold in Celsius, type:

```
apc> tempHigh C
E000: Success
21 C
```

Example 3: To view the high-temperature threshold of guest Rack PDU 2 in Fahrenheit, type:

```
apc> tempHigh 2:F
E000: Success
85 F
```

tempMax

Access: Administrator, Device User

Description: Set or view the max-temperature threshold in either Fahrenheit or Celsius.

Example 1: To set the max-temperature threshold to 80º Fahrenheit, type:

```
apc> tempMax F 80
E000: Success
```

Example 2: To view the max-temperature threshold in Celsius, type:

```
apc> tempMax C
E000: Success
27 C
```

Example 3: To view the max-temperature threshold in Fahrenheit, type:

```
apc> tempMax F
E000: Success
80 F
```

tempReading

Access: Administrator, Device User

Description: View the temperature value in either Fahrenheit or Celsius from the sensor.

Example 1: To view the temperature value in Fahrenheit, type:

```
apc> tempReading F
E000: Success
51.1 F
```

Example 2: To view the temperature value of guest Rack PDU 3 in Celsius, type:

```
apc> tempReading 2:C
E000: Success
23.5 C
```

whoami

Access: Administrator, Device User

Description: View the user name of the active user.

Example:

```
apc> whoami
E000: Success
admin
```

Web Interface

Supported Web Browsers

You can use Microsoft® Internet Explorer® (IE) 7.x and higher (on Windows® operating systems only) or Mozilla® Firefox® 3.0.6 or higher (on all operating systems) to access the Rack PDU through its Web interface. Other commonly available browsers may work but have not been fully tested by APC.

The Rack PDU cannot work with a proxy server. Before you can use a Web browser to access the Web interface of the Rack PDU, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Rack PDU.
- Configure the proxy server so that it does not proxy the specific IP address of the Rack PDU.

Logging On to the Web Interface

Overview

You can use the DNS name or System IP address of the Rack PDU for the URL address of the Web interface. Use your case-sensitive user name and password to log on. The default user names follow and differ by account type:

- **apc** for an Administrator
- **device** for a Device User
- **readonly** for a Read-Only User

The default password is **apc** for all three account types.

Note: If you are using HTTPS (SSL/TLS) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the Rack PDU. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

For information about the Web page displayed when you log on, see “About the Home Tab” on page 46.

URL address formats

Type the DNS name or IP address of the Rack PDU in the Web browser's URL address field and press ENTER. When you specify a non-default Web server port in Internet Explorer, you must include `http://` or `https://` in the URL.

Common browser error messages at log-on.

Error Message	Browser	Cause of the Error
"You are not authorized to view this page" or "Someone is currently logged in..."	Internet Explorer, Firefox	Someone else is logged on
"This page cannot be displayed."	Internet Explorer	Web access is disabled, or the URL was not correct.
"Unable to connect."	Firefox	

URL format examples.

- For a DNS name of Web1:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (HTTP with SSL) is your access mode
- For a System IP address of 139.225.6.133 and the default Web server port (80):
  - `http://139.225.6.133` if HTTP is your access mode
  - `https//139.225.6.133` if HTTPS (HTTP with SSL) is your access mode
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
  - `http://139.225.6.133:5000` if HTTP is your access mode
  - `https://139.225.6.133:5000` if HTTPS (HTTP with SSL) is your access mode
- For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default Web server port (5000):
  - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode

Web Interface Features

Read the following to familiarize yourself with basic Web interface features for your Rack PDU.

Tabs

The following tabs are available:

- **Home**: Appears when you log on. View active alarms, the load status of the **Rack PDU**, and the most recent Rack PDU events. For more information, see “About the Home Tab” on page 46.
- **Device Manager**: View the load status for the Rack PDU, configure load thresholds, and view and manage the peak load measurement. For more information, see “About the Device Manager Tab” on page 47.
- **Environment**: View temperature and humidity sensor data, if a sensor is connected to the **Rack PDU**.
- **Logs**: View event, data, and system logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Device status icons

One or more icons and accompanying text indicate the current operating status of the Rack PDU:

Symbol	Description
	Critical: A critical alarm exists, which requires immediate action.
	Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	No Alarms: No alarms are present, and the Rack PDU and NMC are operating normally.

At the upper right corner of every page, the Web interface displays the same icons currently displayed on the **Home** page to report Rack PDU status:

- The **No Alarms** icon if no alarms exist.
- One or both of the other icons (**Critical** and **Warning**) if any alarms exist, and after each icon, the number of active alarms of that severity.

To return to the **Home** tab to view its summary of the Rack PDU status, including the active alarms, click a quick status icon on any page of the interface.

Quick Links

At the lower left on each page of the interface, there are three configurable links. By default, the links access the URLs for these Web pages:

- **Link 1**: The home page of the APC Web site
- **Link 2**: Demonstrations of APC Web-enabled products
- **Link 3:** Information on APC Remote Monitoring Services.
  To reconfigure the links, see “Configure Links” on page 79.

Other Web interface features

- The IP address appears in the upper left corner.
- A context-sensitive **Help** link and **Log off** link are located in the upper right corner.

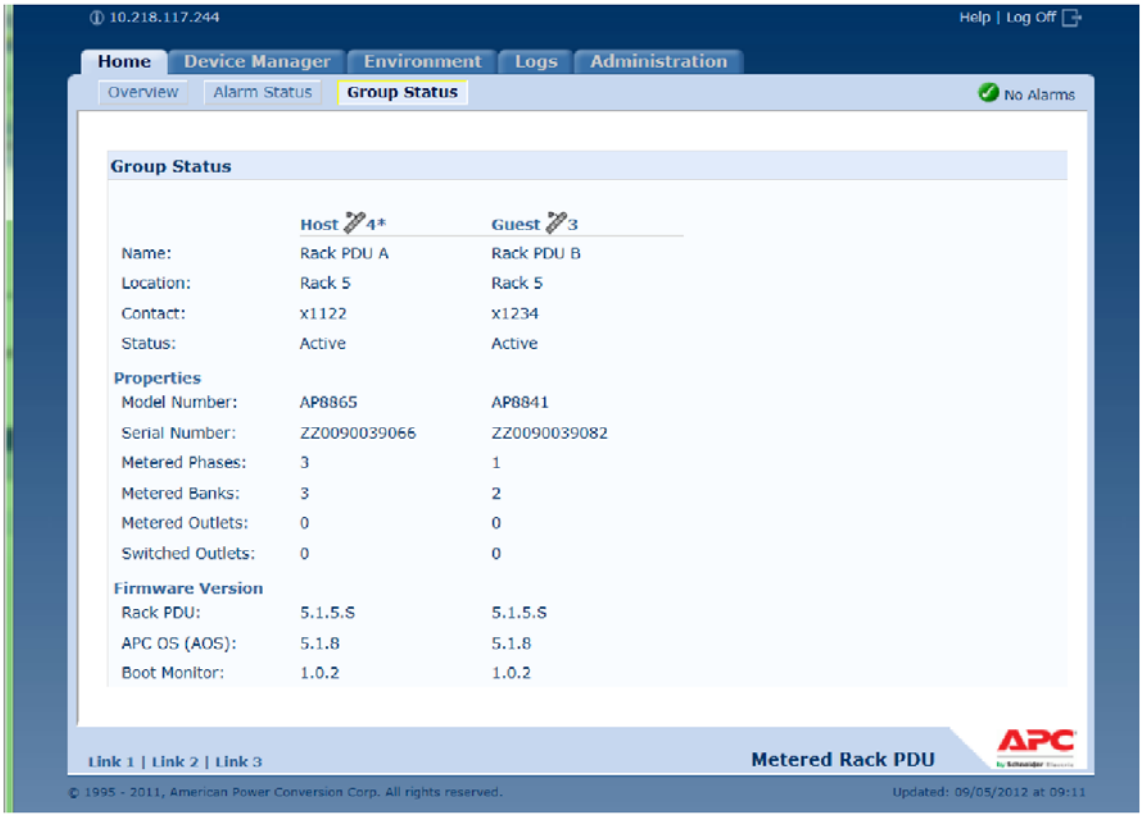
Network Port Sharing on the Web Interface

Group Control using Network Port Sharing

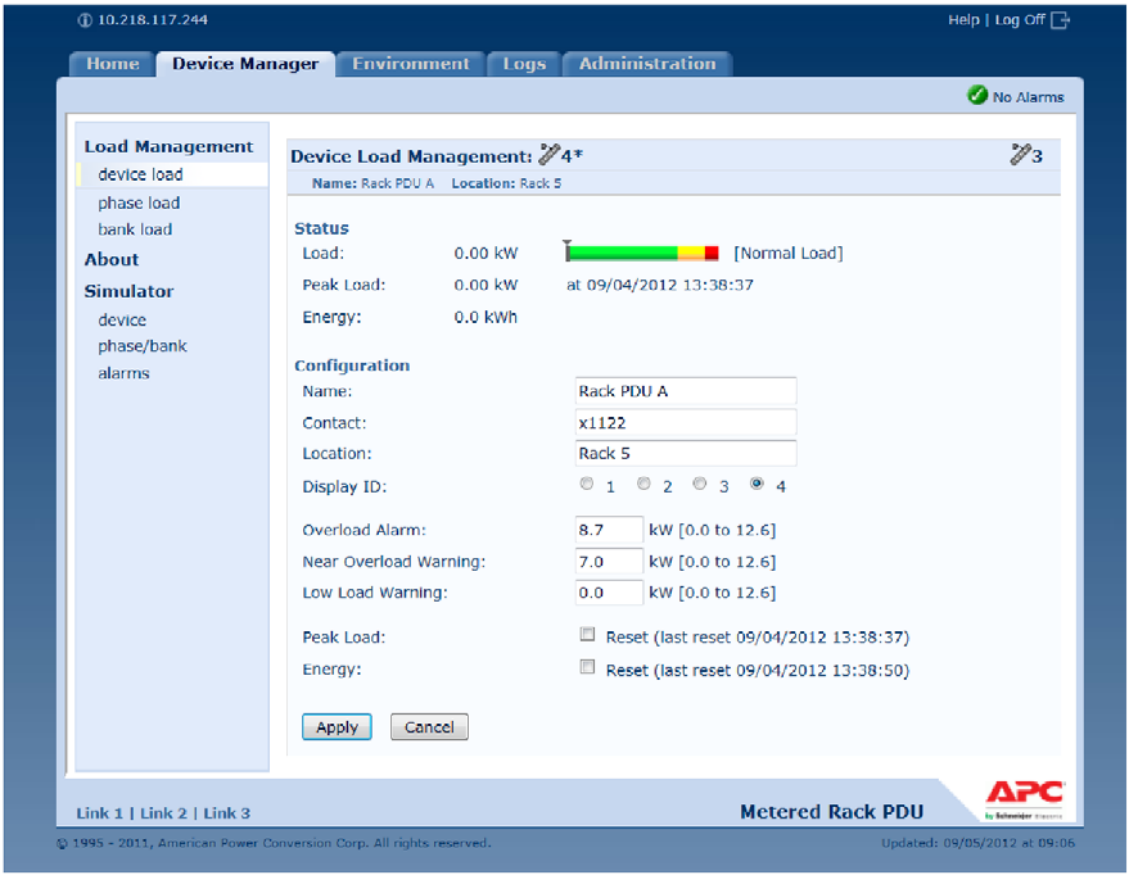
The web interface of the Rack PDU will have additional capabilities if the Rack PDU is part of a group. These capabilities are only displayed if the Rack PDU is part of a group. This includes a "Group Status" page, and the ability to select which Rack PDU to view data from.

The Group Status page lists basic information for the Host Rack PDU and any connected guests. Guests are denoted using a Rack PDU icon and the Display ID.

Information on the Group Status page includes name, location, contact, basic model properties, firmware revision information, and group communication status of each Rack PDU. In addition, the Group Status page allows the user to remove any Rack PDUs that have been removed from the group and are in a lost communication state.



Most of the web pages under the Home, Device Manager, and Environment tabs allow you to switch between Rack PDUs for viewing status and configuration/control. This switching is accomplished by selecting the Rack PDU Display ID of the unit you would like to view. This is located at the top right of each table that supports multiple Rack PDUs. The Host Rack PDU that you are logged into is always denoted with an asterisk (*) following the Display ID.



Note: The Reset/Reboot web page has many additional reset/reboot options for Rack PDU groups. These include individual Rack PDU reset to defaults, individual Rack PDU rebooting, and clearing of guest PDU lost communication alarms by removing the guests from the group.

About the Home Tab

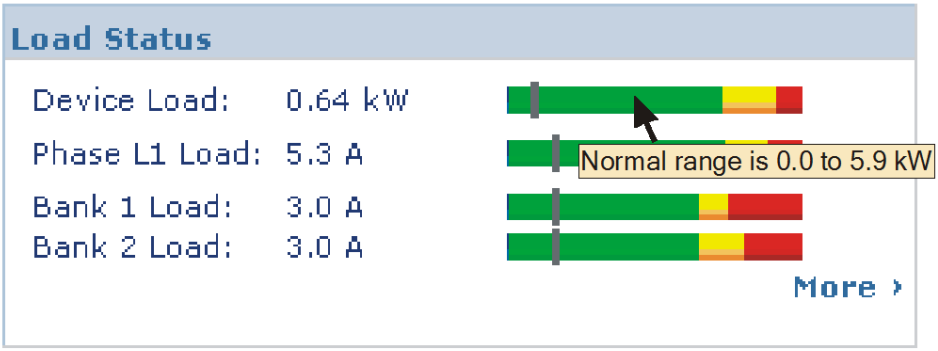
Use the **Home** tab to view active alarms, the load status of the Rack PDU, and the most recent Rack PDU events.

The Overview view

Path: Home > Overview

The top of the **Overview** indicates the alarm status. If one or more alarms are present, the number and type of alarms are indicated with a link to the **Alarm Status** view, where you can view descriptions of each alarm. If no alarms exist, the Overview displays, “No Alarms Present.”

In the **Load Status** area, view the load for the device in kW and for the phases and banks in amps, as applicable. The green, yellow, and red meter shows the current load status: normal, near overload, or overload. Note that if a low load threshold was configured the meter will also include a blue segment to the left of the green. Hover over the colors to view the configured load thresholds.



Click **More** to go to the **Device Manager** tab to configure thresholds and to view and manage peak load information.

In the device parameters area, view the name, contact, location, current rating, type of user account accessing the Rack PDU, and the amount of time the Rack PDU has been operating since the last reboot from either a power cycle or a reboot of the Management Interface. [For more information, see “Reset the Rack PDU” on page 78.]

In the **Recent Device Events** area, view, in reverse chronological order, the events that occurred most recently and the dates and times they occurred. A maximum of five events are shown at one time. Click **More Events** to go to the **Logs** tab to view the entire event log.

The Alarm Status view

Path: Home > Alarm Status

The **Alarm Status** view provides a description of all alarms present. For details about a temperature or humidity threshold violation, click the Environment tab.

Device Management

About the Device Manager Tab

Path: Device Manager

Use the **Device Manager** tab to:

- View the load status for the Rack PDU
- Configure load thresholds for all connected devices, phases, and banks as applicable
- Configure a name and location for the Rack PDU
- View and manage the peak load measurement

Viewing the Load Status and Peak Load

Path: Device Manager > *Load Management options*

Use the **Load Management** menu options to view the load for the device, phases, and banks. The indicator in the green, yellow, and red meter shows the current load status: normal, near overload, or overload. If a low load threshold was configured, the meter will include a blue segment to the left of the green. When viewing the **Device Load**, the triangle above the meter indicates peak load.

Configuring Load Thresholds

Path: Device Manager > *Load Management options*

Note: The Rack PDU generates an alarm when any bank exceeds its rated value. However, if a circuit breaker trips, there is no definitive indication that the circuit breaker is open, other than that the current for that bank will drop. Set the **Low Load Warning Threshold** to **1 amp** for these reasons:

- The default setting for the **Low Load Warning Threshold** is 0 amps. This effectively disables the warning. With a setting of 0 amps for the **Low Load Warning Threshold**, the Web interface will not indicate that a circuit breaker may have tripped.
- A 1-amp detection threshold for the Low Load Warning for Bank Load Management will help to indicate that a circuit breaker may have tripped.

To configure load thresholds:

1. Click the **Device Manager** tab.
2. To configure load thresholds for the device, phases, or banks, make a selection from the **Load Management** menu.
3. Set **Overload Alarm**, **Near Overload Warning**, and **Low Load Warning** thresholds.
4. Click **Apply**.

Configure the Name and Location of the Rack PDU

Path: Device Manager > Device Load

The name and location you enter appear on the **Home** tab.

Note: You can set the Name and Location through either the Device Manager tab or the Administration tab. A change in one affects the other.

1. Click the **Device Manager** tab, then **device load** from the **Load Management** menu.
2. Enter a name and location.
3. Click **Apply**.

Resetting Peak Load and kWh

Path: Device Manager > Device Load

1. Click the **Device Manager** tab, then **device load** from the **Load Management** menu.
2. Click the **Peak Load** and **Kilowatt-Hours** check boxes as desired.
3. Click **Apply**.

Environment

Configure Temperature and Humidity Sensors

Path: Environment

Through the **Environment** tab, when you have a temperature or a temperature and humidity sensor connected to the Rack PDU, you can set thresholds for Warning and Critical alarm generation (see “Device status icons” on page 42 for details on each type of alarm).

For temperature:

- If the high temperature threshold is reached, the system generates a Warning alarm.
- If the maximum temperature threshold is reached, the system generates a Critical alarm.

Similarly, for humidity:

- If the low humidity threshold is reached, the system generates a Warning alarm.
- If the minimum humidity threshold is reached, the system generates a Critical alarm.

  Note: Click the thermometer symbol in the upper right corner to toggle between Fahrenheit and Celsius.

To configure temperature and humidity sensors:

1. Enter values for minimum, maximum, high, and low thresholds.
2. Enter **Hysteresis** values. (See “Hysteresis” on page 49 for details.)
3. Enable alarm generation as desired.
4. Click **Apply**.

Hysteresis. This value specifies how far past a threshold the temperature or humidity must return to clear a threshold violation.

- For Maximum and High temperature threshold violations, the clearing point is the threshold minus the hysteresis.
- For Minimum and Low humidity threshold violations, the clearing point is the threshold plus the hysteresis.

Increase the value for Temperature Hysteresis or Humidity Hysteresis to avoid multiple alarms if temperature or humidity that has caused a violation then wavers slightly up and down. If the hysteresis value is too low, such wavering can cause and clear a threshold violation repeatedly.

Example of rising but wavering temperature: The maximum temperature threshold is 85°F, and the temperature hysteresis is 3°F. The temperature rises above 85°F, violating the threshold. It then wavers down to 84°F and then up to 86°F repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the temperature would have to drop to 82°F (3°F below the threshold).

Example of falling but wavering humidity: The minimum humidity threshold is 18%, and the humidity hysteresis is 8%. The humidity falls below 18%, violating the threshold. It then wavers up to 24% and down to 13% repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the humidity would have to rise to above 26% (8% past the threshold).

Logs

Use the Event and Data Logs

Event log

Path: Logs > Events > *options*

You can view, filter, or delete the event log. By default, the log displays all events recorded during the last two days in reverse chronological order.

For lists of all configurable events and their current configuration, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu. See “Configuring by event” on page 70.

To display the event log (Logs > Events > log):

- By default, view the event log as a page of the Web interface. The most recent event is recorded on page 1. In the navigation bar below the log:
  - Click a page number to open a specific page of the log.
  - Click **Previous** or **Next** to view the events recorded immediately before or after the events listed on the open page.
  - Click << to return to the first page or click >> to view the last page of the log.
- To see the listed events on one page, click **Launch Log in New Window** from the event log page to display a full-screen view of the log.

  Note: In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button.

You can also use FTP or Secure CoPy (SCP) to view the event log. See “How to use FTP or SCP to retrieve log files” on page 54.

To filter the log (Logs > Events > log):

- **Filtering the log by date or time:** To display the entire event log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the Rack PDU restarts.

  To display events logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display events, then click **Apply**. The filter configuration is saved until the Rack PDU restarts.

- **Filtering the log by event**: To specify the events that display in the log, click **Filter Log**. Clear the checkbox of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active.
  As Administrator, click **Save As Default** to save this filter as the default log view for all users. If you do not click **Save As Default**, the filter is active until you clear it or until the Rack PDU restarts.
  To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.

  Note: Events are processed through the filter using **OR** logic.
  Events that you do not select from the **Filter By Severity** list never display in the filtered event log, even if the event occurs in a category you selected from the **Filter by Category** list.
  Events that you do not select from the **Filter by Category** list never display in the filtered event log, even if devices in the category enter an alarm state you selected from the **Filter by Severity** list.

To delete the log (Logs > Events > log):

To delete all events recorded in the log, click **Clear Log** on the Web page that displays the log. Deleted events cannot be retrieved. To disable the logging of events based on their assigned severity level or their event category, see “Configuring by event” on page 70.

To configure reverse lookup (Logs > Events > reverse lookup):

Reverse lookup is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

To resize the event log (Logs > Events > size):

By default, the event log stores 400 events. You can change the number of events the log stores. When you resize the event log, all existing log entries are deleted. To avoid losing log data, use FTP or SCP to retrieve the log before you enter a new value in the **Event Log Size** field. See “How to use FTP or SCP to retrieve log files” on page 54.
When the log is full, the older entries are deleted.

Network Port Sharing Event Logs and Traps.

Rack PDU events from guest PDUs are sent to the host PDU for inclusion into its log. The log entry will include the Display ID of the unit that the event occurred on.
These events are then handled the same as local events from the host PDU. Therefore alarms, SNMP traps, e-mails, Syslog, etc will support Rack PDU events and alarms from all Rack PDUs in a group.

Example event log: Rack PDU 4: Device low load.

Note: System events will only be logged for the host PDU. System events from guest PDUs will not be logged on the host PDU.

Data log

Path: Logs > Data > *options*

The data log records the current and power for the device, phase, and banks, as well as temperature and humidity at the specified time interval. Each entry is listed by the date and time the data was recorded.

To display the data log (Logs > Data > log):

- By default, view the data log as a page of the Web interface. The most recent data item is recorded on page 1. From the navigation menu below the log:
  - Click a page number to open a specific page of the log.
  - Click **Previous** or **Next** to view the data recorded immediately before or after the data that is listed on the open page.
  - Click << to return to the first page of the log, or click >> to view the last page of the log.
- To see the listed data on one page, click **Launch Log in New Window** from the data log page to display a full-screen view of the log.

  Note: In your browser's options, JavaScript must be enabled for you to use the **Launch Log in New Window** button.

Alternatively, you can use FTP or SCP to view the data log. See “How to use FTP or SCP to retrieve log files” on page 54.

To filter the log by date or time (Logs > Data > log):

To display the entire data log or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the device restarts.

To display data logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display data, then click **Apply**. The filter configuration is saved until the device restarts.

To delete the data log:

To delete all data recorded in the log, click **Clear Data Log** on the Web page that displays the log. Deleted data cannot be retrieved.

To set the data collection interval (Logs > Data > interval):

Define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log, and view the calculation of how many days of data the log can store, based on the interval you selected. When the log is full, the older entries are deleted. To avoid automatic deletion of older data, enable and configure data log rotation, described in the next section.

To configure data log rotation (Logs > Data > rotation):

Set up a password-protected data log repository on a specified FTP server. Enabling rotation causes the contents of the data log to be appended to the file you specify by name and location. Updates to this file occur at the upload interval you specify.

Parameter	Description
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server Address	The location of the FTP server where the data repository file is stored.
User Name	The user name required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
Password	The password required to send data to the repository file.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file).
Delay *X* hours between uploads	The number of hours between uploads of data to the file.
Upload every *X* minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to *X* times	The maximum number of times the upload will be attempted after an initial failure.
Until Upload Succeeds	Attempt to upload the file until the transfer is completed.

To resize the data log (Logs > Data > size):

By default, the data log stores 500 records. You can change the number of records the log stores. When you resize the data log, all existing log records are deleted. To avoid losing records, use FTP or SCP to retrieve the log before you enter a new value in the **Data Log Size** field. See “How to use FTP or SCP to retrieve log files” on page 54.

When the log is full, the older entries are deleted.

Network Port Sharing Data Log:

The host Rack PDU will poll data from guest PDUs so that data from all PDUs in a group are available. To view data from a different Rack PDU in a group, select the desired Rack PDU from the "Filter Log" pull-down list.

Similarly for data log graphing, you can select a different Rack PDU by clicking on the "Change Data Filter" button.

How to use FTP or SCP to retrieve log files

An Administrator or Device User can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) and import it into a spreadsheet.

- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the Rack PDU
  - The unique **Event Code** for each recorded event (*event.txt* file only)

    Note: The Rack PDU uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file.

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

See the *Security Handbook*, available at **www.apc.com**, for information on available protocols and methods for setting up the type of security you need.

To use SCP to retrieve the files. To use SCP to retrieve the *event.txt* file:

`scp` ***username@hostname_or_ip_address***`:event.txt ./event.txt`

To use SCP to retrieve the *data.txt* file, use the following command:

`scp` ***username@hostname_or_ip_address***`:data.txt ./data.txt`

To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the IP address of the Rack PDU, and press ENTER.

   If the **Port** setting for the **FTP Server** option (set through the **Network** menu of the **Administration** tab) has been changed from its default (**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 set a non-default port value to enhance security for the FTP Server, see “FTP Server” on page 68. You can specify any port from 5001 to 32768.
2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **apc** is the default for **User Name** and **Password**. For the Device User, the defaults are **device** for **User Name** and **apc** for **Password**.
3. Use the **get** command to transmit the text of a log to your local drive.
   `ftp>get event.txt`

   or

   `ftp>get data.txt`
4. Type `quit` at the `ftp>` prompt to exit from FTP.

Administration: Security

Local Users

Setting user access

Path: Administration > Security > Local Users > *options*

The Administrator user account always has access to the Rack PDU.

The Device User and Read-Only User accounts are enabled by default. To disable the Device User or Read-Only User accounts, select the user account from the left navigation menu, then clear the **Enable** checkbox.

You set the case-sensitive user name and password for each account type in the same manner. Maximum length is 64 characters for a user name and 64 characters for a password. Blank passwords (passwords with no characters) are not allowed.

For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see “Types of User Accounts” on page 2.

Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web interface and command line interface
Device User	device	apc	
Read-Only User	readonly	apc	Web interface only

Remote Users

Authentication

Path: Administration > Security > Remote Users > Authentication Method

Use this option to select how to administer remote access to the Rack PDU.

For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook*, available at **www.apc.com**.

The authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service) is supported.

- When a user accesses the Rack PDU or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the User permission level.
- RADIUS user names used with the Rack PDU are limited to 32 characters.

Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

  Note: If **RADIUS Only** is selected, and the RADIUS server is unavailable, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the command line interface and change the **access** setting to **local** or **radiusLocal** to regain access. For example, the command to change the access setting to **local** would be: **radius -a local**

RADIUS

Path: Administration > Security > Remote Users > RADIUS

Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the Rack PDU and the time-out period for each.
- Click on a link, and configure the parameters for authentication by a new RADIUS server.
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	Definition
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Click on a link to configure the server. Note:RADIUS servers use port 1812 by default to authenticate users. Non-standard ports are currently unsupported.
Secret	The shared secret between the RADIUS server and the Rack PDU.
Timeout	The time in seconds that the Rack PDU waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.

Configure the RADIUS Server

Summary of the configuration procedure

You must configure your RADIUS server to work with the Rack PDU.

For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see the *Security Handbook*.

1. Add the IP address of the Rack PDU to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the Web interface only).

   See your RADIUS server documentation for information about the RADIUS users file, and see the *Security Handbook* for an example.

3. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs require a dictionary entry and a RADIUS users file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will fail. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX® with shadow passwords

If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS "user" file. To allow only Device Users, change the APC-Service-Type to `Device`.

```
DEFAULT     Auth-Type = System
            APC-Service-Type = Admin
```

- Add user names and attributes to the RADIUS "user" file, and verify the password against /etc/passwd. The following example is for users `bconners` and `thawk`:

```
bconners    Auth-Type = System
            APC-Service-Type = Admin
thawk       Auth-Type = System
            APC-Service-Type = Device
```

Supported RADIUS servers

FreeRADIUS and Microsoft IAS 2003 are supported. Other commonly available RADIUS applications may work but have not been fully tested.

RADIUS and Network Port Sharing

Note: See the Security Handbook for APC Network Management Cards for more information on using RADIUS.

Inactivity Timeout

Path: Administration > Security > Auto Log Off

Use this option to configure the time (3 minutes by default) that the system waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

Note: This timer continues to run if a user closes the browser window without first logging off by clicking **Log Off** at the upper right. Because that user is still considered to be logged on, no user can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a user closes the browser window without logging off, no user can log on for 3 minutes.

Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings

Path: Administration > Network > TCP/IP

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the Rack PDU. For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

Setting	Description
Enable	Enable or disable IPv4 with this check box.
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack PDU requests network assignment from any BOOTP server: • If the Rack PDU receives a valid response, it starts the network services. • If the Rack PDU finds a BOOTP server, but a request to that server fails or times out, the Rack PDU stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and the Rack PDU receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail :[1] • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	The default setting. At 32-second intervals, the Rack PDU requests network assignment from any DHCP server. • If the Rack PDU receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services. • If the Rack PDU finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.[1] • **Require vendor specific cookie to accept DHCP Address**: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the Rack PDU.

[1.] The default values for these three settings on the configuration pages generally do not need to be changed:
- **Vendor Class**: APC
- **Client ID**: The MAC address of the Rack PDU, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

DHCP response options

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

Vendor Specific Information (option 43). The Rack PDU uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains an APC-specific options in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default.

- **APC Cookie. Tag 1, Len 4, Data "1APC"**

  Option 43 communicates to the Rack PDU that a DHCP server is configured to service devices.

  Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

  ```
  Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
  ```

TCP/IP options. The Rack PDU uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in **RFC2132**.

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131)**: The IP address that the DHCP server is leasing to the Rack PDU.
- **Subnet Mask** (option 1): The Subnet Mask value that the Rack PDU needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the Rack PDU needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Rack PDU.
- **Renewal Time, T1** (option 58): The time that the Rack PDU 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 Rack PDU must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. The Rack PDU also uses these options within a valid DHCP response. All of these options except the last are described in **RFC2132**.

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the Rack PDU can use.
- **Time Offset** (option 2): The offset of the Rack PDU's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the Rack PDU can use.
- **Host Name** (option 12): The host name that the Rack PDU will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Rack PDU will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Rack PDU will download the .ini file. After the download, the .ini file is used as a boot file to reconfigure the settings.

Path: Administration > Network > TCP/IP > IPv6 settings

Setting	Description
Enable	Enable or disable IPv6 with this check box.
Manual	Configure IPv6 manually by entering the IP address and the default gateway.
Auto Configuration	When the Auto Configuration check box is selected, the system obtains addressing prefixes from the router (if available). It uses those prefixes to automatically configure IPv6 addresses.
DHCPv6 Mode	**Router Controlled**: Selecting this option means that DHCPv6 is controlled by the Managed(M) and Other(O) flags received in IPv6 router advertisements. When a router advertisement is received, the NMC checks whether the M or the O flag is set. The NMC interprets the state of the M (Managed Address Configuration Flag) and O (Other Stateful Configuration Flag) "bits" for the following cases: • *Neither is set*: Indicates the local network has no DHCPv6 infrastructure. The NMC uses router advertisements and manual configuration to get addresses that are not link-local and other settings. • *M, or M and O are set*: In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed. This is true even if subsequent router advertisement packets are received in which the M flag is not set. If an O flag is received first, then an M flag is received subsequently, the NMC performs full address configuration upon receipt of the M flag • *Only O is set*: In this situation, the NMC sends a DHCPv6 Info-Request packet. DHCPv6 will be used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`. **Address and Other Information:** With this radio box selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. **Non-Address Information Only**: With this radio box selected, DHCPv6 will be used to configure "other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`. **Never**: Select this to disable DHCPv6.

Port Speed

Path: Administration > Network > Port Speed

The **Port Speed** setting defines the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
- Alternatively, you can choose 10 Mbps or 100 Mbps, each with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

Ping Response

Path: Administration > Network > Ping Response

- Select the Enable check box for **IPv4 Ping Response** to allow the NMC to respond to network pings. Clear the check box to disable an NMC response. This does not apply to IPv6.

DNS

Path: Administration > Network > DNS > *options*

Use the options under **DNS** to configure and test the Domain Name System (DNS):

- Select **Primary DNS Server** or **Secondary DNS Server** to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the Rack PDU to send e-mail, you must at least define the IP address of the primary DNS server.
  - The Rack PDU waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the Rack PDU does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the Rack PDU or on a nearby segment (but not across a wide-area network [WAN]).
  - Define the IP addresses of the DNS servers then enter the DNS name of a computer on your network to look up the IP address for that computer to verify correct operation.
- **Host Name**: Configure a host name here and a domain name in the **Domain Name** field then users can enter a host name in any field in the NMC interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4)**: Configure the domain name here only. In all other fields in the NMC interface (except e-mail addresses) that accept domain names, the NMC adds this domain name when only a host name is entered.
  - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
  - To override the expansion of a specific host name entry, include a trailing period. The NMC recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6)**: Specify the IPv6 domain name here.
- Select **test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Type**, select the method to use for the DNS query:
    - **by Host**: the URL name of the server
    - **by FQDN**: the fully-qualified domain name
    - **by IP**: the IP address of the server
    - **by MX**: the Mail Exchange used by the server
  - As **Query Question**, identify the value to be used for the selected query type:

Query Type Selected	Query Question to Use
by Host	The URL
by FQDN	The fully qualified domain name, *`my_server.my_domain`*
by IP	The IP address
by MX	The Mail Exchange address

  - View the result of the test DNS request in the **Last Query Response** field.

Web

Path: Administration > Network > Web > *options*

Option	Description

access	To activate changes to any of these selections, log off from the Rack PDU:
	• **Disable**: Disables access to the Web interface. (To re-enable access, log in to the command line interface, then type the command `http -S enable`. For HTTPS access, type `https -S enable`.)
	• **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Rack PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon.
	
	See "Creating and Installing Digital Certificates" in the *Security Handbook*, available at **www.apc.com**.
	
	HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the Rack PDU.
	
	HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack PDU.
	
	For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/ssl** on the Rack PDU. • **Generating**: The Rack PDU is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the Rack PDU. • **Valid certificate**: A valid certificate was installed or was generated by the Rack PDU. Click on this link to view the contents of the certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the** Rack PDU **generates a default certificate, a process which delays access to the interface for up to one minute.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See "Creating and Installing Digital Certificates" in the *Security Handbook*, available at **www.apc.com**, to choose a method for using digital certificates created by the Security Wizard or generated by the Rack PDU. **Remove**: Delete the current certificate.

Console

Path: Administration > Network > Console > *options*

Option	Description

access	Choose one of the following for access by Telnet or Secure SHell (SSH):
	• **Disable**: Disables all access to the command line interface.
	• **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH**: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission.
	
	Configure the ports to be used by these protocols:
	• **Telnet Port**: The Telnet port used to communicate with the Rack PDU (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port**: The SSH port used to communicate with the Rack PDU (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.

ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key. • **Generating**: The Rack PDU is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Rack PDU. • **Valid**: One of the following valid host keys is in the **/ssh** directory (the required location on the Rack PDU): •A 1024-bit or 2048-bit host key created by the Security Wizard •A 2048-bit RSA host key generated by the Rack PDU **Add or Replace**: Browse to and upload a host key file created by the Security Wizard. To use the APC Security Wizard, see the *Security Handbook, available* at **www.apc.com**. Note:To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the** Rack PDU **takes up to one minute to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

Note: To use SSH, you must have an SSH client installed. Most Linux and other UNIX platforms include an SSH client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

SNMP

All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When using StruxureWare Data Center Expert to manage a Rack PDU on the public network of an StruxureWare Data Center Expert system, you must have SNMP enabled in the Rack PDU interface. Read access will allow the StruxureWare Data Center Expert device to receive traps from the Rack PDU, but Write access is required while you use the interface of the Rack PDU to set the StruxureWare Data Center Expert device as a trap receiver.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at **www.apc.com.**

Network Port Sharing.

All Rack PDUs in a group can be accessed through the Host Rack PDU via SNMP "rPDU2" OIDs available in our PowerNet-MIB.
The full path to these OIDs is:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).apc(318).products(1).hardware(1).rPDU2(26)

Individual Rack PDUs can be identified in the SNMP MIB tables by viewing the corresponding "Module" OIDs in each table. These Module OIDs will return the Display ID of the Rack PDU.

Example Module OIDs: rPDU2IdentModule, rPDU2DeviceConfigModule, rPDU2SensorTempHumidityConfigModule

In order to be backwards compatible with previous versions, the Host Rack PDU will always be the first index in any table that supports multiple Rack PDUs. In addition, after the Rack PDU group is set up, the index order of guest Rack PDUs should not change even if the Display ID is changed or a PDU temporarily loses communication. The index order should only change if you manually remove a Rack PDU from the group.

An MIB table walk should skip the indexes associated with a Rack PDU that has temporarily lost communication.

SNMPv1

Path: Administration > Network > SNMPv1 > *options*

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
access control	You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IPv4 and IPv6 addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that an NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are `public`, `private`, `public2`, and `private2`. **NMS IP/Host Name:** The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or command line interface. • **Write+**: GETS and SETS at any time. • **Disable**: No GETS or SETS at any time.

SNMPv3

Path: Administration > Network > SNMPv3 > *options*

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

Note: To use SNMPv3, you must have a MIB program that supports SNMPv3.
The Rack PDU supports SHA or MD5 authentication and AES or DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.
user profiles	By default, lists the settings of four user profiles, configured with the user names **apc snmp profile1** through **apc snmp profile4**, and no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters (`apc auth passphrase`, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase of 15 to 32 ASCII characters (`apc crypt passphrase`, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3. **Authentication Protocol:** The APC implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected. **Privacy Protocol:** The implementation of SNMPv3 supports AES and DES as the protocols for encrypting and decrypting data. Privacy of transmitted data requires that a privacy protocol is selected and that a privacy passphrase is provided in the request from the NMS. When a privacy protocol is enabled but the NMS does not provide a privacy passphrase, the SNMP request is not encrypted. **Note:** You cannot select the privacy protocol if no authentication protocol is selected.

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. To edit the access control settings for a user profile, click its user name. **Access:** Mark the **Enable** checkbox to activate the access control specified by the parameters in this access control entry. **User Name:** From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the **user profiles** option on the left navigation menu. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server

Path: Administration > Network > FTP Server

The **FTP Server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the Rack PDU. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.

Note: FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with SCP. Selecting and configuring Secure SHell (SSH) enables SCP automatically.
At any time that you want a Rack PDU to be accessible for management by StruxureWare Data Center Expert, FTP Server must be enabled in the Rack PDU interface.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at **www.apc.com**.

Administration: Notification

Event Actions

Path: Administration > Notification > Event Actions > *options*

Types of notification

You can configure event actions to occur in response to an event or group of events. These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - APC Remote Monitoring Service
  - Syslog notification
- Indirect notification
  - Event log. If no direct notification is configured, users must check the log to determine which events have occurred

    You can also log system performance data to use for device monitoring. See “Data log” on page 52 for information on how to configure and use this data logging option.
  - Queries (SNMP GETs)

    For more information, see “SNMP” on page 65. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

Notification parameters. For events that have an associated clearing event, you can also set the following parameters as you configure events individually or by group, as described in the next two sections. To access the parameters, click the receiver or recipient name.

Parameter	Description
Delay x time before sending	If the event persists for the specified time, a notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of *x* time	The notification is sent at the specified interval (e.g., every 2 minutes).
Up to *x* times	During an active event, the notification repeats for this number of times.
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

Configuring by event. To define event actions for an individual event:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. In the list of events, review the marked columns to see whether the action you want is already configured. (By default, logging is configured for all events.)
3. To view or change the current configuration, such as recipients to be notified by e-mail or paging, or Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name.

   Note: If no Syslog server is configured, items related to Syslog configuration are not displayed.

   When viewing details of an event's configuration, you can change the configuration, enable or disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers, but you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:

   - "Identifying Syslog servers" on page 74
   - "E-mail recipients" on page 71
   - "Trap Receivers" on page 73

Configuring by group. To configure a group of events simultaneously:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how to group events for configuration:
   - Choose **Grouped by severity**, and then select all events of one or more severity levels. You cannot change the severity of an event.
   - Choose **Grouped by category**, and then select all events in one or more pre-defined categories.
3. Click **Next>>** to move from page to page to do the following:
   a. Select event actions for the group of events.
      - To choose any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
      - If you choose **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** (or both) on the next page.

   b. Select whether to leave the newly configured event action enabled for this group of events or to disable the action.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers. (See “DNS” on page 62.)
- The IP address or DNS name for **SMTP Server** and **From Address.** (See “SMTP” on page 71.)
- The e-mail addresses for a maximum of four recipients. (See “E-mail recipients” on page 71.)

  Note: You can use the **To Address** setting of the **recipients** option to send e-mail to a text-based mobile device.

SMTP.

Path: Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IPv4/IPv6 address or DNS name of the local SMTP server. Note:This definition is required only when **SMTP Server** is set to **Local**. See “E-mail recipients” on page 71.
From Address	The contents of the **From** field in e-mail messages sent by the Rack PDU: • In the format *user@* [*IP_address*] (if an IP address is specified as **Local SMTP Server**) • In the format *user@domain* (if DNS is configured and the DNS name is specified as **Local SMTP Server**) in the e-mail messages. Note:The local SMTP server may require that you use a valid user account on the server for this setting. See the server’s documentation.

E-mail recipients.

Path: Administration > Notification > E-mail > recipients

Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient’s pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. To bypass the DNS lookup of the mail server’s IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. Note:The recipient’s pager must be able to use text-based messaging.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.

Setting	Description

SMTP Server	Select one of the following methods for routing e-mail:
	• **Local**: Through the Rack PDU's SMTP server. This setting (recommended) ensures that the e-mail is sent before the Rack PDU's 20-second time-out, and, if necessary, is retried several times. Also do one of the following:
	  • Enable forwarding at the Rack PDU's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding.
	  • Set up a special e-mail account for the Rack PDU to forward e-mail to an external mail account.
	• **Recipient**: Directly to the recipient's SMTP server. With this setting, the Rack PDU tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent.
	
	When the recipient uses the Rack PDU's SMTP server, this setting has no effect.

Format	The long format contains Name, Location, Contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
Language	Choose a language from the drop-down list and any mails will be sent in that language. It is possible to use different languages for different users.
User Name Password Confirm Password	If your mail server requires authentication, type your user name and password here. This performs a simple authentication, not SSI.

E-mail test.

Path: Administration > Notification > E-mail > test

Send a test message to a configured recipient.

SNMP traps

Trap Receivers.

Path: Administration > Notification > SNMP Traps > trap receivers

View trap receivers by NMS IP/Host Name. You can configure up to six trap receivers.

- To configure a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select either the SNMPv1 or SNMPv3 radio button. For an NMS to receive both types of traps, you must configure two trap receivers for that NMS, one for each trap type.

Item	Definition
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IPv4/IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.
Language	Choose a language from the drop-down list. This can differ from the UI and from other trap receivers.

SNMPv1 option.

Item	Definition
Community Name	The name (`public` by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
Authenticate Traps	When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device). To disable that ability, unmark the checkbox.

SNMPv3 option. Select the identifier of the user profile for this trap receiver. (To view the settings of the user profiles identified by the user names selectable here, choose **Network** on the top menu bar and **user profiles** under **SNMPv3** on the left navigation menu.)

See “SNMPv3” on page 67 for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test

Path: Administration > Notification > SNMP Traps > test

Last Test Result. The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

To. Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration page is displayed.

Remote Monitoring Service

Path: Administration > Notification > Remote Monitoring

The APC Remote Monitoring Service (RMS) is an optional service that monitors your system from a remote operation center 24 hours a day, 7 days a week, and notifies you of device and system events.

To purchase the APC RMS service, contact your vendor or click on the link on the top part of this screen page: **APC RMS Web site**.

Registration. To activate RMS for the Rack PDU, select **Enable APC Remote Monitoring Service.,** choose between **Register Company and Device** and **Register Device Only**, complete the form, and click **Send APC RMS Registration**.

Use the **Reset APC Remote Monitoring Service Registration** check box to discontinue the service, whether permanently or temporarily (for example, if you are moving a Rack PDU).

Syslog

Path: Logs > Syslog > *options*

The Rack PDU can send messages to up to four Syslog servers when an event occurs. The Syslog servers record events that occur at network devices in a log that provides a centralized record of events.

This User guide does not describe Syslog or its configuration values in detail. See **RFC3164** for more information about Syslog.

Identifying Syslog servers.

Path: Logs > Syslog > servers

Setting	Definition
Syslog Server	Uses IPv4/IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the Rack PDU.
Port	The user datagram protocol (UDP) port that the Rack PDU will use to send Syslog messages. The default is **514**, the UDP port assigned to Syslog.
Protocol	Choose between UDP and TCP.
Language	Choose the language for any Syslog messages.

Syslog settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Rack PDU's Syslog messages (**User**, by default). Note:**User** best defines the Syslog messages sent by the Rack PDU. **Do not** change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of Rack PDU or Environment events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** Note:To disable Syslog messages, see "Configuring event actions" on page 69.

Syslog test and format example.

Path: Logs > Syslog > test

Send a test message to the Syslog servers configured through the **servers** option.

1. Select a severity to assign to the test message.
2. Define the test message, according to the required message fields
   – The priority (PRI): the Syslog priority assigned to the message's event, and the facility code of messages sent by the Rack PDU.
   – The Header: a time stamp and the IP address of the Rack PDU.
   – The message (MSG) part:
      • The TAG field, followed by a colon and space, identifies the event type.
      • The CONTENT field is the event text, followed (optionally) by a space and the event code.

      For example, `APC: Test Syslog` is valid.

Administration: General Options

Identification

Path: Administration > General > Identification

Define the **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by StruxureWare Data Center Expert and the SNMP agent of the Rack PDU. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

For more information about MIB-II OIDs, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide*, available at **www.apc.com**.

The **Name** and **Location** fields also identify the device when you register for APC Remote Monitoring Service. See “Remote Monitoring Service” on page 74.

Set the Date and Time

Mode

Path: Administration > General > Date & Time > mode

Set the time and date used by the Rack PDU. You can change the current settings manually or through a Network Time Protocol (NTP) Server:

- **Manual Mode**: Do one of the following:
  - Enter the date and time for the Rack PDU.
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using.
- **Synchronize with NTP Server**: Have an NTP Server define the date and time for the Rack PDU.

  Note: By default, any Rack PDU on the private side of the StruxureWare Data Center Expert obtains its time settings by using StruxureWare Data Center Expert as an NTP server.

Setting	Definition
Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time.
Update Interval	Define how often, in hours, the Rack PDU accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of the date and time by the NTP Server.

Daylight saving

Path: Administration > General > Date & Time > daylight saving

Enable traditional United States Daylight Saving Time (DST), or enable and configure a customized daylight saving time to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time (DST):

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g, the fourth Sunday), choose **Fourth/Last**. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose **Fifth/Last**.

Format

Path: Administration > General > Date & Time > date format

Select the numerical format in which to display all dates in this user interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

Use an .ini File

Path: Administration > General > User Config File

Use the settings from one Rack PDU to configure another. Retrieve the config.ini file from the configured Rack PDU, customize that file (e.g., change the IP address), and upload the customized file to the new Rack PDU. The file name can be up to 64 characters, and must have the.ini suffix.

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Rack PDU can use it to set its own configuration.

To retrieve and customize the file of a configured Rack PDU, see “How to Export Configuration Settings” on page 82.

Instead of uploading the file to one Rack PDU, you can export the file to multiple Rack PDUs by using an FTP or SCP script.

Event Log and Temperature Units

Path: Administration > General > Preferences

Color-code event log text

This option is disabled by default. Mark the **Event Log Color Coding** checkbox to enable color-coding of alarm text recorded in the event log. System-event entries and configuration-change entries do not change color.

Text Color	Alarm Severity
Red	**Critical**: A critical alarm exists, which requires immediate action.
Orange	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
Green	**Alarm Cleared**: The conditions that caused the alarm have improved.
Black	**Normal**: No alarms are present. The Rack PDU and all connected devices are operating normally.

Change the default temperature scale

Select the temperature scale (Fahrenheit or Celsius) in which to display all temperature measurements in this user interface.

Reset the Rack PDU

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the Rack PDU.
Reset All[1]	Clear the **Exclude TCP/IP** checkbox to reset all configuration values; mark the **Exclude TCP/IP** checkbox to reset all values except TCP/IP.
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the Rack PDU receive its TCP/IP settings from a DHCP or BOOTP server. See “TCP/IP and Communication Settings” on page 59.
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
	RPDU to Defaults: Resets only Rack PDU settings, not network settings, to their defaults.
1. Resetting may take up to a minute.	

Configure Links

Path: Administration > General > Quick Links

Select the **Administration** tab, **General** on the top menu bar, and **Quick Links** on the left navigation menu to view and change the URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **Link 1**: The home page of the APC Web site.
- **Link 2**: A page where you can use samples of Web-enabled products.
- **Link 3**: The home page of the Schneider Electric Remote Monitoring Service.

To reconfigure any of the following, click the link name in the **Display** column:

- **Display**: The short link name displayed on each interface page
- **Name**: A name that fully identifies the target or purpose of the link
- **Address**: Any URL—for example, the URL of another device or server

About the Rack PDU

Path: Administration > General > About

The hardware information is useful to APC Customer Support for troubleshooting problems with the Rack PDU. The serial number and MAC address are also available on the Rack PDU itself.

Firmware information for the Application Module, APC OS (AOS), and APC Boot Monitor indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at the APC Web site.

Management Uptime is the length of time the interface has been running continuously.

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

The Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more Rack PDUs or network-enabled devices (devices containing an embedded APC Network Management Card [NMC]). You can use the Wizard in either of the following ways:

- Remotely over your TCP/IP network to discover and configure unconfigured Rack PDUs or devices on the same network segment as the computer running the Wizard.
- Through a direct connection from a serial port of your computer to a Rack PDU or device to configure or reconfigure it.

System requirements

Version 5.0.0 or higher of the Wizard runs on Microsoft Windows 2000, Windows Server® 2003, Windows Server® 2008 Windows XP, Windows Vista, and Windows 7.

Installation

To install the Wizard from a downloaded executable file:

1. Go to **www.apc/tools/download**.
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder to which you downloaded it.

Use the Wizard

Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured Rack PDUs.

Launch the Wizard

The installation creates a shortcut link in the **Start** menu to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured Rack PDUs or network-enabled devices, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.) The MAC address can be found:
    - On a label on the device
    - On the Quality Assurance slip that came with the Rack PDU or device

Run the Wizard to perform the configuration. To discover and configure the unconfigured Rack PDUs or network-enabled devices over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first Rack PDU or network-enabled device that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the system IP, subnet mask, and default gateway for the Rack PDU or device identified by the MAC address. Click **Next >**.

   On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Rack PDU or device after the Wizard transmits the settings.
4. Click **Finish** to transmit the settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. If the Wizard finds another unconfigured Rack PDU or device, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the Rack PDU or device whose MAC address is currently displayed, click **Cancel**.

Configure or reconfigure the TCP/IP settings locally

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the provided serial configuration cable (APC part number 940-0144A) from an available communications port on your computer to the serial port of the Rack PDU or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the Rack PDU or network-enabled device is not configured, wait for the Wizard to detect it. Otherwise, click **Next >**.
5. Select **Locally (through the serial port)**, and click **Next >**.
6. Enter the system IP, subnet mask, and default gateway for the Rack PDU or device, and click **Next >**.
7. On the **Transmit Current Settings Remotely** screen, if you select **Start a Web browser when finished**, the default Web browser connects to the Rack PDU or device after the Wizard transmits the settings.
8. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
9. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the Rack PDU or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a Rack PDU and export it to another Rack PDU or to multiple Rack PDUs.

1. Configure a Rack PDU to have the settings you want to export.
2. Retrieve the .ini file from that Rack PDU.
3. Customize the file to change at least the TCP/IP settings.
4. Use a file transfer protocol supported by the Rack PDU to transfer a copy to one or more other Rack PDUs. For a transfer to multiple Rack PDUs, use an FTP or SCP script or the .ini file utility.

Each receiving Rack PDU uses the file to reconfigure its own settings and then deletes it.

Contents of the .ini file

The config.ini file you retrieve from a Rack PDU contains the following:

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific Rack PDU settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values. For example, in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Rack PDU) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

INI and Network Port Sharing

The INI configuration utility is able to get and set values for all Rack PDUs in a group. In order to be backwards compatible, the host Rack PDU will always be designated as first, "PDU_A". Any guest Rack PDUs are then designated "PDU_B", "PDU_C", and "PDU_D" based on their Display ID in ascending order. Therefore, "PDU_A" will not necessarily correlate to Display ID 1, and so on.

Note: Because of the large number of configuration values possible in a Rack PDU group, it may take a very long time to process an INI file set. For example, a Rack PDU group of 4 units with all values changing may take 30 minutes to complete processing.

Detailed procedures

Retrieving. To set up and retrieve an .ini file to export:

1. If possible, use the interface of a Rack PDU to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured Rack PDU:
   a. Open a connection to the Rack PDU, using its IP address:

      ```
      ftp> open ip_address
      ```

   b. Log on using the Administrator user name and password.
   c. Retrieve the config.ini file containing the Rack PDU's settings:

      ```
      ftp> get config.ini
      ```

      The file is written to the folder from which you launched FTP.

      To retrieve configuration settings from multiple Rack PDUs and export them to other Rack PDUs, see *Release Notes: ini File Utility, version 2.0*, available at **www.apc.com**.

Customizing. You must customize the file before you export it.

1. Use a text editor to customize the file.
   – Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   – Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   – Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   – To export scheduled events, configure the values directly in the .ini file.
   – To export a system time with the greatest accuracy, if the receiving Rack PDUs can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

      ```
      NTPEnable=enabled
      ```

      Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
   – To add comments, start each comment line with a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   – The file name can have up to 64 characters and must have the .ini suffix.
   – Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

Transferring the file to a single Rack PDU. To transfer the .ini file to another Rack PDU, do either of the following:

- From the Web interface of the receiving Rack PDU, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the file, or use **Browse**.
- Use any file transfer protocol supported by Rack PDUs, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:

  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the Rack PDU to which you are exporting the .ini file:

  ```
  ftp> open ip_address
  ```

  b. Export the copy of the customized .ini file to the root directory of the receiving Rack PDU:

  ```
  ftp> put filename.ini
  ```

Exporting the file to multiple Rack PDUs. To export the .ini file to multiple Rack PDUs:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Rack PDU.
- Use a batch processing file and the .ini file utility.

  To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0*, available at **www.apc.com**.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Rack PDU completes using the .ini file to update its settings.

`Configuration file upload complete, with` *`number`* `valid values`

If a keyword, section name, or value is invalid, the upload by the receiving Rack PDU succeeds, and additional event text states the error.

Event text	Description
Configuration file warning: Invalid keyword on line *number.* Configuration file warning: Invalid value on line *number.*	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number.*	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A Rack PDU from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack PDU is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

`Rack PDU not discovered`

If you did not intend to export the Rack PDU configuration as part of the .ini file import, ignore these messages.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values. See “Contents of the .ini file” on page 82 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Rack PDUs, ignore these error messages. To prevent these error messages, delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the APC Device IP Configuration Wizard to update the basic TCP/IP settings of the Rack PDU and configure other settings through its user interface. See “Device IP Configuration Wizard” on page 80.

File Transfers

How to Upgrade Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Rack PDU:

- You obtain 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 Rack PDUs support the same features in the same manner.

Firmware module files (Rack PDU)

A firmware release has three modules, and they *must* be upgraded (that is, placed on the Rack PDU) in this order:

- a boot monitor (**bootmon**) module
- an American Power Conversion Operating System (**AOS**) module
- an **application** module

(Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption).

The boot monitor module, the AOS, and the application file names share the same basic format:

`apc_hardware-version_type_firmware-version.bin`

- `apc`: Indicates the context.
- `hardware-version: hw0n` where n identifies the hardware version on which you can use this file.
- `type`: Identifies which module.
- `version`: The version number of the file.
- `bin`: Indicates that this is a binary file.

Firmware File Transfer Methods

Note: Upgrade the bootmon module first, then the AOS module, and finally, the application module by placing them on the Rack PDU in that order.

Obtain the free, latest firmware version from **www.apcc.com/tools/download**. To upgrade the firmware of one or more Rack PDUs, use 1 of these 5 methods:

- On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from the APC Web site. See “Using the Firmware Upgrade Utility” .
- On any supported operating system, use **FTP or SCP** to transfer the individual AOS and application firmware modules. See “Use FTP or SCP to upgrade one Rack PDU” .
- For a Rack PDU that is NOT on your network, use **XMODEM** through a serial connection to transfer the individual firmware modules from your computer to the Rack PDU.
  See “Use XMODEM to upgrade one Rack PDU” .
- Use a **USB drive** to transfer the individual firmware modules from your computer. See “How to upgrade multiple Rack PDUs” .
- For upgrades to multiple Rack PDUs, see “Upgrading the firmware on multiple Rack PDUs” and “Using the Firmware Upgrade Utility for multiple upgrades on Windows”.

Using the Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on the APC Web site. (*Never* use an Upgrade Utility designated for one product to upgrade the firmware of another product).

Using the Utility for upgrades on Windows systems. On any supported Windows operating system, the Firmware Upgrade Utility automates the transferring of the firmware modules, *in the correct module order.* The utility only works with a Rack PDU that has an IPv4 address.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details.

Using the Utility for manual upgrades, primarily on Linux. On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the Rack PDU. See "Firmware File Transfer Methods" for the different upgrade methods after extraction.

To extract the firmware files:

1. After extracting files from the downloaded firmware upgrade file, run the **Firmware Upgrade Utility** (the .exe file).
2. At the prompts, click **Next**>, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

Use FTP or SCP to upgrade one Rack PDU

FTP. To use FTP to upgrade a Rack PDU over the network:

- The Rack PDU must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the Rack PDU, see "FTP Server" on page 68.

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. The firmware module files must be extracted, see "To extract the firmware files:" .
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:
   ```
   C:\>cd apc
   C:\apc>dir
   ```
   For file information, see "Firmware module files (Rack PDU)" on page 86.
3. Open an FTP client session:
   ```
   C:\apc>ftp
   ```
4. Type `open` with the **IP address** of the Rack PDU, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.
   - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):
     ```
     ftp> open 150.250.6.10 21000
     ```
   - Some FTP clients require a colon instead before the port number.
5. Log on as Administrator (**apc** is the default user name and password).
6. Upgrade the AOS. (Always upgrade the AOS before the application module).
   ```
   ftp> bin
   ftp> put apc_hw05_aos_nnn.bin
   ```
   (where *nnn* is the firmware version number)
7. When FTP confirms the transfer, type `quit` to close the session.
8. After 20 seconds, repeat step 3 through step 7, using the application module file name at step 6, .

SCP. To use Secure CoPy (SCP) to upgrade firmware for the Rack PDU, follow these steps (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Locate the firmware modules, see “Using the Utility for manual upgrades, primarily on Linux.” .
2. Use an SCP command line to transfer the AOS firmware module to the Rack PDU. The following example uses *nnn* to represent the version number of the AOS module:

   `scp apc_hw05_aos_`*`nnn`*`.bin apc@158.205.6.185:apc_hw05_aos_`*`nnn`*`.bin`

3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the Rack PDU. (Always upgrade the AOS before the application module).

Use XMODEM to upgrade one Rack PDU

To use XMODEM to upgrade one Rack PDU that is not on the network, you must extract the firmware files from the Firmware Upgrade Utility (see “To extract the firmware files:”).

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0144) to the selected port and to the RJ-12 style serial port at the Rack PDU.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the Rack PDU, then immediately press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press ENTER.
6. From the terminal program’s menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.

   (Always upgrade the AOS before the application module).

7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type `reset` or press the **Reset** button to restart the Rack PDU.

How to upgrade multiple Rack PDUs

Firmware Upgrade Utility. Use this for multiple firmware updates in IPv4 if you have Windows. The utility records all upgrade steps in a log as a good reference to validate the upgrade.

Export configuration settings. You can create batch files and use a utility to retrieve configuration settings from multiple Rack PDUs and export them to other Rack PDUs. See *Release Notes: ini File Utility, version 2.0*, available at **www.apc.com**.

Use FTP or SCP to upgrade multiple Rack PDUs. To upgrade multiple Rack PDUs using an FTP client or using SCP, write a script which automatically performs the procedure.

Using the Firmware Upgrade Utility for multiple upgrades

After downloading from the APC website, double click on the .exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your Rack PDU firmware:

1. Type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify an IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. This should list any device IP, user name, and password, for example,
   ```
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc
   ```
   The new utility works fine with any existing `iplist.txt` file that you have used with the old version of the utility.
3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file. Clear this check box to upgrade the firmware using the IP, user name and password you typed on the dialog box.
4. Choose the **Upgrade Now** button to start the firmware version update(s).
5. Choose **View Log** to verify any upgrade.

Using a USB flash drive to upgrade one Rack PDU

Note: Some flash drives are not compatible with the Rack PDU.

Note: When using a USB flash drive to perform a firmware upgrade load the boot monitor first, then the APC operating system module, and finally, the application module.

If you are unsure whether to upgrade any particular module, then upgrading all three is recommended.

1. Obtain the latest firmware files. See “To extract the firmware files:” on page 87.
2. Create a folder on your flash drive called **apcfirm**.
3. From the latest firmware files that you downloaded, add to the **apcfirm** folder the binary files for the firmware modules that you would like to upgrade. Examples of the binary files for the three firmware modules follow:

Firmware Module	Binary File
APC Boot Monitor	apc_hw0x_bootmon_xxx.bin
APC Operating System (AOS)	apc_hw0x_aos_xxx.bin
Application Module	apc_hw0x_rpdu2g_xxx.bin

4. Use a text editor such as Microsoft Notepad to create a file called **upload.rcf**. Add to the file a line for each firmware module that you want to upgrade as shown below:
```
BM=apc_hw0x_bootmon_xxx.bin
AOS=apc_hw0x_aos_xxx.bin
APP=apc_hw0x_rpdu2g_xxx.bin
```
5. Add the **upload.rcf** file to the **apcfirm** folder on the flash drive.
6. Connect the flash drive to the USB port on the Rack PDU.
7. Either cycle power or press the **Reset** button for the upgrade process to begin.
8. Wait for two to three minutes for the upgrade to complete. When complete, the Rack PDU display will show the firmware version for three seconds and then will resume normal operation, at which time you can remove the flash drive.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the `xferStatus` command in the command line interface to view the last transfer result, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

Code	Description
Successful	The file transfer was successful.
Result not available	There are no recorded file transfers.
Failure unknown	The last file transfer failed for an unknown reason.
Server inaccessible	The TFTP or FTP server could not be found on the network.
Server access denied	The TFTP or FTP server denied access.
File not found	The TFTP or FTP server could not locate the requested file.
File type unknown	The file was downloaded but the contents were not recognized.
File corrupt	The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed.

Verify the version numbers of installed firmware.

Use the Web interface to verify the versions of the upgraded firmware modules by selecting the **Administration** tab, **General** on the top menu bar, and **About** on the left navigation menu, or use an SNMP GET to the MIB II **sysDescr** OID. In the command line interface, use the `about` command.

Troubleshooting

Rack PDU Access Problems

For problems that persist or are not described here, see the back cover of this manual.

Problem	Solution
Unable to ping the Rack PDU	If the Rack PDU's Status LED is green, try to ping another node on the same network segment as the Rack PDU. If that fails, it is not a problem with the Rack PDU. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify all network connections. • Verify the IP addresses of the Rack PDU and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Rack PDU, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Rack PDU's subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the Rack PDU, you must shut down any application, service, or program using the communications port.
Cannot access the command line interface through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the command line interface remotely	• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet. • For SSH, the Rack PDU may be creating a host key. The Rack PDU can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Rack PDU. SSL requires **https**, not **http**, at the beginning of the URL. • Verify that you can ping the Rack PDU. • Verify that you are using a Web browser supported for the Rack PDU. See "Supported Web Browsers" on page 40. • If the Rack PDU has just restarted and SSL security is being set up, the Rack PDU may be generating a server certificate. The Rack PDU can take up to one minute to create this certificate, and the SSL server is not available during that time.
Cannot communicate using Network Port Sharing	• If you are having communications problems with Network Port Sharing, check that the total length of network cable between up to four units is not more than 10 meters. • If you are having communications problems with Network Port Sharing, check that a terminator is installed at both ends of up to four units that can be grouped together. • If you are using Network Port Sharing and do not see one or more of the units in the group, check that all units in the group are using the same firmware revision. You can download appropriate firmware revisions from the APC website.

Appendix A: List of Supported Commands

Network Management Card Command Descriptions

?

about

alarmcount
[-p [all | warning | critical]]

boot
[-b <dhcpBootp | dhcp | bootp | manual>]
[-a <remainDhcpBootp | gotoDhcpOrBootp>]
[-o <stop | prevSettings>]
[-f <retry then fail #>]
[-c <dhcp cookie> [enable | disable]]
[-s <retry then stop #>]
[-v <vendor class>]
[-i <client id>]
[-u <user class>]

cd

date
[-d <“datestring”>]
[-t <00:00:00>]
[-f [mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd]]

delete

dir

eventlog

exit

format

ftp
[-p <port number>]
[-S <enable | disable>]

help

netstat

ping
[<IP address or DNS name>]

portspeed
[-s [auto | 10H | 10F | 100H | 100F]]

prompt
[-s [long | short]]

quit

radius
[-a <local | radiusLocal | radius> (Access)]
[-p1 <primary server>]
[-s1 <primary server secret>]
[-t1 <primary server timeout>]
[-p2 <secondary server>]
[-s2 <secondary server secret>]
[-t2 <secondary server timeout>]reboot

reboot

resetToDef
[-p [all | keepip]]

snmp
[-S <disable | enable>]

snmpv3
[-S <disable | enable>]

system
[-n <system name>]
[-c <system contact>]
[-l <system location>]

tcpip
[-i <IP address>]
[-s <subnet mask>]
[-g <gateway>]
[-d <domain name>]
[-h <host name>]

tcpip6
[-S <enable | disable>] (enables IPv6)
[-i <ipv6 address>] (sets manual IPv6 address)
[-g <ipv6 gateway>] (sets IPv6 gateway)
[-man <enable | disable>] (enables IPv6 manual address)
[-auto <enable | disable>] (enables IPv6 autoconfiguation)
[-d6 <router | stateful | stateless | never>] (sets DHCPv6 mode)

user
[-an <Administrator name>]
[-dn <Device User name>]
[-rn <Read-Only User name>]
[-ap <Administrator password>]
[-dp <Device User password>]
[-rp <Read-Only User password>]
[-t <inactivity timeout in minutes>]

web
[-S <disable | http | https>]
[-ph <http port #>]
[-ps <https port #>]

xferINI

xferStatus

Device Command Descriptions

bkLowLoad
[[id#:]<“all” | bank#> <current>]

bkNearOver
[[id#:]<“all” | bank#> <current>]

bkOverLoad
[<“all” | bank#> <current>]

bkReading
[[id#:]<“all” | bank#>]

devLowLoad
[[id#:]<power>]

devNearOver
[[id#:]<power>]

devOverLoad
[[id#:]<power>]

devReading
[[id#:]<“power” | “energy”>]

humLow
[[id#:]<humidity>]

humMin
[[id#:]<humidity>]

humReading
[id#:]

phLowLoad
[[id#:]<“all” | phase#> <current>]

phNearOver
[[id#:]<“all” | phase#> <current>]

phOverLoad
[[id#:]<“all” | phase#> <current>]

phReading
[[id#:]<“all” | phase#> <“current” | “voltage” | “power”>]

prodInfo
[id#:]

sensorName
[[id#:]<sensor name>]

tempHigh
[[id#:]<“F” | “C”> <temperature>]

tempMax
[[id#:]<“F” | “C”> <temperature>]

tempReading
[[id#:]<“F” | “C”>]

whoami

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 the APC Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

For information on how to obtain local customer support, contact the APC representative or other distributors from whom you purchased your APC product.

© APC, the APC logo, StruxureWare, and PowerNet are owned by Schneider Electric Industries S.A.S., American Power Conversion Corporation, or their affiliated companies. All other trademarks are property of their respective owners.

990-3429D-001 **10/2012**