USER'S GUIDE
NetworkAIR ACPA4000

Contents

Introduction

Product Description

Features of the Network Management Card

The APC® NetworkAIR® Portable Air Conditioning Unit cools your data center equipment. In addition, a Network Management Card, which supports multiple, open standards such as Telnet, HTTP, HTTPS, SSL, TLS, SCP, and SNMP, provides full management of the ACPA4000. The management card provides management of the following features:

- Temperature and humidity monitoring
- Input contact monitoring for use with dry contact sensors
- Mapping and management of output relays
- Event log accessible by Telnet, FTP, serial connection, SCP, or a Web browser
- SNMP traps and e-mail notifications sent based on the severity level of the events
- Syslog events sent to configured Syslog servers
- Security protocols for authentication and encryption

Initial setup

You must define three TCP/IP settings for the Network Management Card before it can operate on the network.

- IP address of the Network Management Card
- Subnet mask
- IP address of the default gateway

See also

To configure the TCP/IP settings, see the NetworkAIR ACPA 4000 *Installation, Operation, and Maintenance* manual, provided in printed form, and in PDF on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

To use a DHCP server to configure the TCP/IP settings at a Network Management Card, see Boot Mode.

Internal Management Features

Overview

The Network Management Card has two user interfaces (control console, Web interface) which provide menus with options that allow you to manage the ACPA4000, depending on your preferences. You can also manage the ACPA4000 through the SNMP interface by using a SNMP browser with the PowerNet MIB.

For more information about the Network Management Card's user interfaces, see Control Console and Web Interface.

See also

For more information about how to use the PowerNet MIB with an SNMP browser, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\mibguide.pdf**), which is provided on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

Login control

Only one user at a time can log on to the Network Management Card to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the ACPA4000 always has the highest priority
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has the next highest priority
- Web access has the lowest priority either directly or through the InfraStruXure Manager

For information about how SNMP access to the Management Card is controlled, see SNMP.

Types of user accounts

The Network Management Card has three levels of access (Administrator, Device Manager, and Read-Only User), all of which are protected by user name and password requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default user name and password are both **apc**.
- A Device Manager can access only the **Log** option in the **Events** menu and use the **Cooling**, **Inputs/Outputs**, **Alarms**, and **Identification** menus. The Device Manager's 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 menus as a Device Manager, but without the capability to change configurations, control devices, or delete data. Links to configuration options are visible but are disabled, and the event log displays no **Delete** button.

  The Read-only user's default user name is **readonly**, and the default password is **apc**.

To set **User Name** and **Password** values for the Administrator, Device Manager, and Read-only user accounts, see User Manager.

Note

You must use the Web interface to configure values for the Read-only User.

How to Recover from a Lost Password

You can use a local computer, a computer that connects to the ACPA4000 or other device through the serial port, to access the control console.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the APC smart-signaling cable (cable 940-0103) to the selected port on the computer and to the RS-232 serial port on the rear panel of the ACPA4000.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port as follows:
   - 2400 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - 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 on the Network Management Card. The Status LED will flash between orange and green. Immediately press the **Reset** button on the Network Management Card a second time while the LED is flashing to reset the user name and password to their defaults temporarily.

6. Press ENTER as many times as necessary to re-display the **User Name** prompt, 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. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
9. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Upgrading Firmware for the Card

See also

To download a firmware upgrade for your Network Management Card using FTP, see the *Management Card Addendum* (**.\doc\en\addendum.pdf**) on the provided APC NetworkAIR Portable Air Conditioner *Utility* CD.

For you to be able to use FTP to upgrade a single Network Management Card over the network:

- The Network Management Card must be attached to the network.
- The FTP server must be enabled at the Network Management Card.
- The Network Management Card must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Network Management Card firmware:

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

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

   Files listed for a NetworkAIR Portable Air Conditioning Unit, for example, might be the following:

   – `apc_hw02_aos_225.bin`

   – `apc_hw02_nairpa_101.bin`

2. Open an FTP client session:

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

3. Type `open` and the Network Management Card's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu

has changed from its default value of **21**, you must use the non-default value in the FTP command.

a. For some FTP clients, use a colon to add the port number to the end of the IP address.

b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Network Management Card's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to a Network Management Card with an IP address of 150.250.6.10.

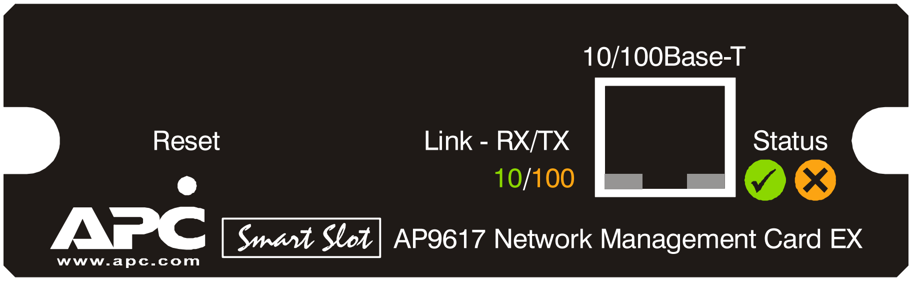
```
ftp> open 150.250.6.10 21000
```

4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. For example:

```
ftp> bin
ftp> put apc_hw02_aos_225.bin
```

6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat **step 2** through **step 6** for the application module. In **step 6**, use the application module file instead of the AOS module.

Network Management Card—Front Panel



Features

Item	Description
Reset Button	Resets the Management Card while the power remains on.
10/100 Base-T Connector	Connects the Management Card to the Ethernet network.
Link-RX/TX (10/100) LED	See Link-RX/TX (10/100) LED.
Status LEDs	See Status LED.

Link-RX/TX (10/100) LED

The Link RX/TX LED on the front of the Network Management Card indicates the network connection status of the card.

Condition	Description
Off	One of the following situations exist: • The Network Management Card is not receiving input power. • The Network Management Card is starting up. • The Network Management Card is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid Green	The device is connected to a network operating at 10 Megabits per second (Mbps).
Solid Orange	The device is connected to a network operating at 100 Megabits per second (Mbps).
Flashing Green	The device is receiving or transmitting data packets at 10 Megabits per second (Mbps).
Flashing Orange	The device is receiving or transmitting data packets at 100 Megabits per second (Mbps).

Status LED

This LED indicates the network status of the Network Management Card.

Condition	Description
Off	The Network Management Card has no power.
Solid Green	The Network Management Card has valid TCP/IP settings.
Flashing Green	The Network Management Card does not have valid TCP/IP settings.[1]
Solid Orange	A hardware failure has been detected in the Network Management Card. Contact APC Worldwide Customer Support.
Flashing Orange	The Network Management Card is making BOOTP[2] requests.
Alternately Flashing Green and Orange	The Network Management Card is making DHCP[3] requests.[1]

[1] If you do not use a BOOTP server, see the NetworkAIR ACPA 4000 *Installation, Operation, and Maintenance* manual provided in printed format and in PDF on the APC NetworkAIR Portable Air Conditioner *Utility* CD to configure the TCP/IP settings.

[2] To use a BOOTP server, see the *Management Card Addendum* on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

[3] To use a DHCP server, see Boot Mode.

Watchdog Features

Overview

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

Network interface watchdog mechanism

The Network Management Card implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Network Management Card 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 itself.

Resetting the network timer

To ensure that the Network Management Card does not restart if the network is quiet for 9.5 minutes, the Network Management Card attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Network Management Card, and that 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 most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Network Management Card from restarting.

Control Console

How to Log On

Overview

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

Use case-sensitive **User Name** and **Password** entries to log on (by default, **apc** and **apc**, for an Administrator, or **device** and **apc**, for a Device Manager). A Read-Only User has no access to the control console.

If you cannot remember your user name or password, see How to Recover from a Lost Password.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

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 control console from any computer on the same subnet:

1. At a command prompt, type `telnet` and the System IP address for the ACPA4000 (when the PDU uses the default telnet port of 23), and then press ENTER. For example:

   ```
   telnet 139.225.6.133
   ```

   Note If the Network Management Card uses a non-default port number (between 5000 and 32767), you need to include a colon or a space (depending on your Telnet client) after the IP address and then the port number.

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

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords, and transmitted data.

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

Local access to the control console

You can use a local computer that connects to the ACPA4000 through the serial port on the rear panel of the unit.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied serial cable (940-0103) to connect the selected port to the serial port on the rear panel of the ACPA4000.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER twice to display the **User Name** prompt.

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at a Network Management Card.

```
User Name : apc
Password  : ***


American Power Conversion               Network Management Card AOS v2.2.5
(c) Copyright 2003 All Rights Reserved  NetworkAIR PA APP           v1.0.1
-------------------------------------------------------------------------------
Name      : NetworkAIR PA                              Date : 02/07/2004
Contact   : Bill Cooper                                Time : 10:16:58
Location  : Testing Lab                                User : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes                  Stat : P+ N+ A+

Communication Established
------- Control Console -------------------------------------------------------

     1- Device Manager
     2- Network
     3- System
     4- Logout

<ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log

>
```

Information and status fields

Main screen information fields.

- 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. On the Example main screen, the application firmware for the ACPA4000 is displayed.

```
Network Management Card AOS         v2.2.5
NetworkAIR PA APP                   v1.0.1
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

```
Name       : NetworkAIR PA
Contact    : Bill Cooper
Location   : Testing Lab
```

To set the **Name**, **Contact**, and **Location** values, see Identification.

- An **Up Time** field reports how long the Network Management Card has been running since it was last reset or since power was applied.

```
Up Time    : 0 Days 0 Hours 43 Minutes
```

- Two fields identify the date and time the last time the screen refreshed.

```
Date : 02/07/2004
Time : 10:16:58
```

- A **User** field identifies whether you logged on as Administrator or Device Manager.

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Network Management Card status.

```
Stat : P+ N+ A+
```

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Management Card failed to connect to the network.
N!	Another device is using the IP address of the Network Management Card.
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 the AOS status is not P+, contact APC Worldwide Customer Support, even if you can still access the Network Management Card.

NetworkAIR ACPA4000 status field.

The status field displays the status of the devices in which the card is installed. Under normal operation this field will contain **Communication Established**.

Control Console Menus

Menu structure

The menus in the control console list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

For menus that allow you to change a setting you must use the **Accept Changes** option to save the changes you made.

While in a menu, you can also do the following:

- Type ? and press ENTER to access brief menu option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to go back to the menu from which you accessed the current menu.
- Press CTRL-C to return to the main (control console) menu.
- Press CTRL-L to access the event log.

For information about the event log, see Event-Related Menus.

Main menu

The main control console menu has options that provide access to the management features of the control console:

```
1- Device Manager
2- Network
3- System
4- Logout
```

Device Manager option

This option accesses the **Device Manager** menu. Select the components you want to manage. For more information on these settings see NetworkAIR PA Menus. For example:

```
1- Cooling
2- Inputs
3- Outputs
4- Alarms
5- Identification
6- Display Interface Log
```

Network option

To do any of the following tasks, see Network Menu:

- Configure the Network Management Card's TCP/IP settings.
- Configure the settings for the type of server (DHCP or BOOTP) to be used to provide the TCP/IP settings to the card.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet/SSH, Web interface/SSL, SNMP, E-mail, DNS, and Syslog features of the Network Management Card.

System option

To do any of the following tasks, see System Menu:

- Control **Administrator** and **Device Manager** access
- Define the system **Name**, **Contact**, and **Location** values
- Set the date and time used by the Network Management Card
- Restart the Network Management Card
- Reset control console settings to their default values
- Access System information about the Network Management Card

Logout option

Select the logout option to log out of the control console.

How to Log On

Overview

You can use a Network Management Card's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

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

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

Note

If you are using HTTPS (SSL/TSL) 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, you must use an IP address to log on to the Network Management Card if an IP address was specified as the common name in the certificate, or you must use a DNS name to log on if a DNS name was specified as the common name in the certificate.

For information about the Web page that appears when you log on to the Web interface, see Summary Page.

Supported Web browsers

As your browser, you can use Microsoft® Internet Explorer (IE) 5.0 (and higher) or Netscape® 4.0.8 (and higher, except Netscape 6.*x*) to access the Network Management Card through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

Data verification, the event log, and Message Digest 5 (MD5) authentication require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Network Management Card cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

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

URL address formats

Type the DNS name or IP address of the Network Management Card in the Web browser's URL address field and press ENTER. Except when you specify a non-default web server port in Internet Explorer, `http://` or `https://` is automatically added by the browser.

Note

If the error "You are not authorized to view this page" occurs (Internet Explorer only), another user is logged on to the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the Management Card may use a non-default Web-server port that you did not specify correctly in the address.

For more information, see Web/SSL.

- For a DNS name of Web1, the entry would be one of the following:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Network Management Card uses the default port (80) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133` if HTTP is your access mode
  - `https://139.225.6.133` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Network Management Card uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133:5000` if HTTP is your access mode

– `https://139.225.6.133:5000` if HTTPS (SSL/TLS) is your access mode

Summary Page

Note

Type the Management Card's DNS name or IP address in the Web browser's URL address field, and press ENTER. Except when you specify a non-default web server port in Internet Explorer, http:// or https:// is automatically added by the browser.

When you log on to the Web interface at the Network Management Card, the status view is displayed at the right side of the screen, the quick status tab is displayed at the upper right, and the navigation menu is displayed at the left.

Status

The **Status** view has these sections:

- **Device Status** shows the following:
  - Active alarms for the ACPA4000
  - Temperature and humidity measurements for the ACPA4000
  - State of key components
  - Run hours of key components
- **NetworkAIR PA Series** shows the following:
  - **Name**, **Contact,** and **Location** information for the Network Management Card.
  - Date and Time the screen was last refreshed.
  - **User** type (**Administrator, Device Manage,** or **Read Only**).

Note

The information available in the status view is available on the control console on the **Device Manager** menu, under **Cooling**, then **Status**.

Quick status tab

The quick status tab is displayed in the upper right of every screen in the Web interface. The tab displays a warning of any alarms and provides a link to the online help.

?	Access the online help for the displayed page.
✓	Click the green “device operating normally” icon to return to the status screen where the status for attached devices is displayed.
⚠	Click the “attention required” icon to return to the status screen where active warnings and alarms are displayed.
✖	Click the “alarm detected” icon to return to the status screen where active alarms are displayed.

Navigation frame

Contains the menus that provide access to the available ACPA4000 options.

See Navigation Menu.

Navigation Menu

Overview

When you log on to the Web interface, the navigation menu (left frame) includes the following elements:

- IP address of the Network Management Card
- Network Management Card menus to manage the ACPA4000 and its components
  - **Cooling**
  - **Inputs/Outputs**
  - **Alarms**
  - **Identification**
- Menus to manage the event log, network connection, and system parameters
  - **Events**
  - **Network**
  - **System**

Note When you log on as a Device Manager or Read-only user, the **Network** and **System** menus do not appear in the navigation menu.

- **Logout** option
- **Help** menu
- **Links** menu

Select a menu to perform a task

To do the following, see the Cooling Menu:

- Set the default cooling schedule.
- Set up to eight cooling schedules.
- Set the deadband and start-up delay.
- Change the units of temperature values.

To do the following, see the Inputs/Outputs Menu:

- Set up the Remote Run/Stop input.
- Set up input contacts.
- Map events and inputs to the output relays.

To do the following, see Alarms menu:

- View active alarms for the ACPA4000.
- Set the temperature and humidity thresholds.

To do the following, see Event-Related Menus:

- Access the event log.
- Configure the actions to be taken based on an event's severity level.
- Configure SNMP Trap Receiver settings for sending event-based traps.
- Define who will receive e-mail notifications of events.
- Test e-mail settings.

To do the following, see Network Menu:

- Configure new TCP/IP settings for the Network Management Card.
- Identify the Domain Name Service (DNS) Server and test the network connection to that server.
- Define settings for FTP, Telnet, SSH, the Web interface, SNMP, e-mail, and SSL/TLS.

- Configure the Syslog message feature for the ACPA4000.

To do the following, see System Menu:

- Control **Administrator**, **Device Manager**, and **Read-Only** user access.
- Define the **Name**, **Contact**, and **Location** values.
- Set the date and time used by the ACPA4000.
- Restart the Network Management Card for the NetworkAIR ACPA4000.
- Reset network interface settings to their default settings.
- Define the URL addresses of the user links and APC logo links in the Web interface, as described in Links menu.
- Register for APC's Remote Monitoring (Web interface) Service.

Help menu

When you click **Help**, the contents for all of the online help is displayed. However, from any Web interface pages, you can use the question mark (**?**) in the quick status bar to link to the section of the online help for that page.

The **Help** menu also has an **About System** option you use to view the following items of information about the Network Management Card: Model Number, Serial Number, Hardware Revision, Manufacture Date, MAC Address, Application Module, and APC OS (AOS) Module, including the date and time each of the two modules was created.

Note

In the control console, the **About System** option, which is a **System** menu option, identifies the flash type used.

Links menu

Provides three user-definable URL link options. By default, these links access the following APC Web pages:

- **APC's Web Site** accesses the APC home page.
- **Testdrive Demo** accesses a demonstration page where you can use samples of APC web-enabled products.
- **APC Monitoring** accesses the "APC Remote Monitoring Service" page about pay-for-monitoring services available from APC.

To redefine these links so that they point to other URLs:

1. Click on **Links** in the **System** menu.
2. Define any new names for **User Links**.
3. Define any new URL addresses that you want **User Links** to access. Only HTTP links may be defined.
4. Click **Apply**.

Note The link associated with the APC logo is also definable.

Cooling Menu

Cooling Status and Control

The cooling menus allow you to view and change the settings that the ACPA4000 uses to determine its cooling response.

Web interface. The **Scheduling** section of the **Cooling Control** screen provides the status of the programmable schedules, and lists the schedule that is active.

Click **Configure** to adjust the schedules. Set each option below for the schedules you want to use, and then click **Apply**.

Control Console. In the control console, the Cooling menu has two options, Status and Control. The **Status** screen shows the temperature and humidity readings, and is similar to the Summary Page on the Web interface.

The **Control** screen provides three options which correspond to the options on the web interface:

- **Default Schedule** — Active when no other schedule is active
- **Operating Schedules** — Set the schedules according to the table
- **General Settings** — Same as general settings on the Web interface

After you adjust a schedule or the general settings, select **Accept Changes** to save the change.

Option	**Description**
Schedule	Number that identifies the schedule.
On/Off	State of the schedule. If the schedule is Off, it will not control the unit during the selected times.
Mode	Set the mode to Cooling, Venting, or Off. • **Cooling**: The unit will run the blower fan and cool the air in the room. • **Venting**: The unit will run the blower fan, without cooling the air in the room. • **Off**: The unit will not run the blower fan, or cool the air in the room.
Setpoint	Set the target air temperature for the room.
Blower	Set the speed of the blower. • **High**: The normal speed for cooling or venting. • **Low**: Set the unit to low speed and cooling to achieve limited dehumidification.
Days	Set the days that this schedule will be active. • **Every day**: The schedule will be active every day of the week. • **Weekdays**: The schedule will be active on every day during the week. • **Weekends**: The schedule will be active on every day during the weekend • **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**: The schedule will be active on the day you choose.
Start Time	Set the time for the schedule to start on the selected day. The start time setting uses a 24-hour clock.
Stop Time	Set the time for the schedule to stop on the selected day.The stop time setting uses a 24-hour clock.

Note

If schedules overlap, the schedule with the highest day-priority will run. The priority is:

- Highest: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
- Next Highest: Weekdays, Weekends
- Lowest: Every Day

The **General Settings** section displays the **Deadband**, **Start-up Delay**, and the Daylight Savings Time adjustment setting (**DST Adjust**).

Option	Description
Deadband	The range above the setpoint at which cooling will begin. The unit does not begin to cool until the room temperature is at the setpoint plus the deadband.
Start-up Delay	The unit will delay this amount of time after power is applied, before it begins cooling.
DST Adjust	Set the unit to automatically adjust the clock for daylight savings time.

Inputs/Outputs Menu

Input Contact Status/Configuration

Web interface. The input contact designated as Remote Run/Stop can be set to either normally open or normally closed.

Control console. The input contact designated as Remote Run/Stop is the first contact of the Inputs list. See User Input Contact Status/Configuration.

User Input Contact Status/Configuration

Web interface. View the status of the input contacts. Click **Configure** to change the settings.

Control console. Enter the number of the input contact you want to modify, and press ENTER. Adjust the name and normal state of each contact in the list, and then select **Accept Changes** to save the change.

Option	Description
Number	The number that identifies this input contact.
Name	Set the name for this input contact.
Current State	View the current state of this input contact.
Normal State	Set the normal state for this input contact.

Output Relay Configuration

Output relays allow you to send information about the unit's alarms and events to external devices through normally open or normally closed contacts.

Web interface. Click **Configure** to change the settings for each relay.

Control Console. Select an output number, change the Normal State or Source for each output, and then select **Accept Changes** to save the change.

Option	Description
Number	The number that identifies this input contact.
Source	Map an alarm, event, or state to this relay.
Current State	View the current state of this output relay.
Normal State	Set the normal state for this output relay.

Alarms

Alarm Status

The **Active Alarms** section lists the severity of each alarm and a description.

Alarm Configuration

The Temperature and Humidity section contains the alarm delay and temperature and humidity thresholds.

Web interface. Click **Configure** to change the settings. Click **Apply** to save your changes, after you modify settings.

Control console. Select **Configuration** and the number of the threshold or delay you want to change. When you have finished adjusting settings on this menu, select **Accept Changes** to save the change.

Option	**Description**
Alarm Delay	Set the delay after the unit starts cooling, before an alarm will occur.
Temperature Thresholds	
Supply High	Set the high temperature threshold for the supply sensor.
Supply Low	Set the low temperature threshold for the supply sensor.
Return High	Set the high temperature threshold for the return sensor.
Return Low	Set the low temperature threshold for the return sensor.
Remote High	Set the high temperature threshold for the remote sensor.
Remote Low	Set the low temperature threshold for the remote sensor.
Humidity Thresholds	
Remote High	Set the high humidity threshold for the remote sensor.
Remote Low	Set the low humidity threshold for the remote sensor.

Identification

About Device

The **Identification** section allows you to define contact information for this device.

Web interface. Click **Configure** to change these settings, and click **Apply** to save your changes.

Control console. Select the number of the setting you want to change. When you finish, select **Accept Changes** to save the change.

- Name
- Contact
- Location

The **NetworkAIR PA Model Information** section provides identifying information for the unit:

- Model Number
- Serial Number
- Firmware Revision
- Hardware Revision
- Date of Manufacture

These items are read-only.

Event-Related Menus

Introduction

Overview

The **Events** menu provides access to the options that you use to do the following tasks:

- Access the event log
- Define the actions to be taken when an event occurs, based on the severity level of that event:
  - Event logging
  - Syslog message notification
  - SNMP trap notification
  - E-mail notification

> **Note** You can use only the Web interface to define which events will use which actions, as described in Event Log and How to Configure Individual Events.

- Define up to four Network Management Stations (NMSs) as trap receivers by their IP addresses.
- Define up to four recipients for event notifications by e-mail.

Menu options

In the Web interface, all of the events options are accessed through the **Events** menu.

In the control console, access the available events-related options as follows:

- Use the **Email** option in the **Network** menu to define the SMTP server and e-mail recipients.
- Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers.
- Use `Display Interface Log` on the Device Manager menu to access the log of events available on the display interface for the ACPA4000.
- Use CTRL-L to access the Network Management Card event log from any menu.

For information on the following topics, use these links:

- Event Log
- Event Actions (Web Interface Only)
- Event Recipients
- E-mail Feature
- How to Configure Individual Events

Event Log

Overview

The ACPA4000 supports event-logging for all Network Management Card application firmware modules. To record and display NetworkAIR PA and Network Management Card events, use any of the following to view the event log:

- Web interface
- Control console
- FTP
- SCP

Logged events

By default, the following events are logged:

- Any event that causes an SNMP trap, except for SNMP authentication failures.
- The Network Management Card's abnormal internal system events

To disable the logging of events based on their assigned severity level, use the **Actions** option in the Web interface's **Events** menu.

See Event Actions (Web Interface Only).

Note

Some Network Management Card (System) events do not have a severity level. Even if you disable the event log for all severity levels, events with no severity level will still be logged.

To access a list of the Network Management Card (System) and NetworkAIR PA (Device) events, see Event List page.

Web interface

The **Log** option in the **Events** menu accesses the event log. This log displays all of the events that have been recorded since the log was last deleted, in reverse chronological order. The **Delete Log** button clears all events from the log.

Control console

Press CTRL-L to display up to 300 events from the event log, in reverse chronological order. Use the SPACE BAR to scroll through the recorded events. While viewing the log, type `d` and press ENTER to clear all events from the log.

Note After events are deleted, they cannot be retrieved.

How to use FTP or SCP to retrieve log files

If you are an Administrator, Device Manager, or read-only user, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) that you can import into a spreadsheet application.

- The file reports all of the events recorded since the log was last deleted.
- The file includes information that the event 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 ACPA4000
  - The unique **Event Code** value for each recorded event

Note

The Network Management Card 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 of the year.

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

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

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

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

```
scp username@hosthame_or_ip_address:event txt ./event.txt
```

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

1. At a command prompt, type `ftp` and the ACPA4000's IP address, and press ENTER.
   If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

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

2. Use the case-sensitive user name and password for either an Administrator or a Device Manager user to log on.
   - For Administrator, **apc** is the default for user name and password.
   - For Device Manager, **device** is the default user name, and **apc** is the default password.
   - For the read only user, **readonly** is the default user name, and **apc** is the default password.
3. Use the **get** command to transmit the text-version of the event log to your local drive.

   ```
   ftp>get event.txt
   ```
4. You can use the **del** command to clear the contents of the event log or data log.

   ```
   ftp>del event.txt
   ```

   You will not be asked to confirm the deletion.

   Note If you clear the event log, a new *event.txt* file is created to record the deleted-log event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Display Interface Log

The display interface log provides access to the event log that is available at the display interface on the front panel of an ACPA4000.

1. Select `Display Interface Log` from the Device Manager menu.
2. Select option `View Log`.
3. Enter the number of the event you want to view.
4. Press ENTER to return to the list of events.

Event Actions (Web Interface Only)

Overview

Use the **Actions** option in the **Events** menu to do the following:

- Select which actions will occur for events that have a severity level:
  - **Event Log** selects which severity levels cause an event to be recorded in the event log.

    📖 See Event log action.

  - **Syslog** selects which severity levels cause messages to be sent to Syslog servers to log events.

    📖 See Syslog action.

  - **SNMP Traps** selects which severity levels cause SNMP traps to be generated.

    📖 See SNMP traps action.

  - **Email** selects which severity levels cause e-mail notifications.

    📖 See Email action.

- Click **Details** for a complete list of the NetworkAIR PA (Device) and Network Management Card (System) events that can occur, and then edit the actions that will occur for an individual event.

  📖 See How to Configure Individual Events.

- Click **Hide Details** to return to the **Actions** option.

Severity levels

Except for some Network Management Card (System) events that do not have a severity level, events are assigned a default severity level.

- **Informational**: Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- **Warning:** Indicates an event that may need to be addressed if the condition continues, but which does not require immediate attention.
- **Severe:** Indicates an event that requires immediate attention.

Note Unless resolved, severe Network Management Card and NetworkAIR PA events can cause incorrect operation of the ACPA4000 or its supported equipment, or can result in the loss of environmental control.

Event log action

You can disable the recording of events in the event log. By default, all events are recorded, even events that have no severity level assigned.

Note Even if you disable the event log action for all severity levels, System (management card) events that have no severity level assigned will still be logged.

📖 For more information about this log, see Event Log.

Syslog action

By default, the **Syslog** action is enabled for all events that have a severity level. However, before you can use this feature to send Syslog messages when events occur, you must configure it.

See Syslog.

SNMP traps action

By default, the **SNMP Traps** action is enabled for all events that have a severity level assigned. However, before you can use SNMP traps for event notifications, you must identify the network management stations (NMSs) that will receive the traps by their IP addresses.

Email action

To define up to four NMSs as trap receivers, see Event Recipients.

By default, the **Email** action is enabled for all events that have a severity level assigned. However, before you can use e-mail for event notifications, you must define the e-mail recipients.

See E-mail Feature.

Event Recipients

Overview

The Web interface and control console both have options that allow you to define up to four trap receivers and up to four e-mail addresses to be used when an event occurs that has SNMP traps or e-mail enabled.

See Event Actions (Web Interface Only).

To identify the servers that will receive Syslog messages, see Syslog.

Trap Receiver settings

To access the **Trap Receiver** settings that allow you to define which NMSs will receive traps:

- In the Web interface, use the **Recipients** option in the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu.

Item	Definition
Community Name	This setting defines the password (maximum of 15 characters) used when traps are sent to the NMS identified by the **Receiver NMS IP** setting.
Receiver NMS IP	Identifies by IP address the NMS that will receive traps. If this setting is **0.0.0.0** (the default value), traps will not be sent to any NMS.
Generation (Web interface) Trap Generation (control console)	Enables (by default) or disables the sending of any traps to the NMS identified by the **Receiver NMS IP** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP** setting.

E-mail Feature

Overview

You can 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 secondary Domain Name Service (DNS) servers.

  See DNS servers.

- The DNS name of the SMTP server and the **From Address** setting for SMTP.

  See SMTP settings.

- The e-mail addresses for a maximum of four recipients.

  See Email recipients.

DNS servers

The Network Management Card cannot send any e-mail messages unless the IP address of the primary DNS server is defined.

📖 See DNS.

The Network Management Card will wait a maximum of 15 seconds for a response from the primary or (if specified) the secondary DNS server. If the Management Card does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers that are on the same segment as the Network Management Card or on a nearby segment (but not across a WAN).

Once you define the IP addresses of the DNS servers, verify that DNS is working correctly. Enter the DNS name of a computer on your network to test whether you can look up the IP address for that DNS name.

SMTP settings

The **Email** option in the **Network** menu accesses the following settings:

Setting	Description
SMTP Server	Defines the SMTP server by its DNS name. **NOTE:** This definition is required only when the **SMTP Server** option (see Email recipients) is set to **Local**.
From Address	Defines the contents of the **From** field in the e-mail messages sent by the Network Management Card. **NOTE:** The SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information.

Email recipients

In the Web interface, use the **Recipients** option in the **Events** menu or the **Configure the Email recipients** link in the “Email Configuration” page to identify up to four e-mail recipients. Use the **Email Test** option to send a test message to a configured recipient.

In the control console, use the **Email** option in the **Network** Menu, to access the e-mail recipient settings.

Setting	**Description**
To Address	Defines the user and domain names of the recipient. • 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. For example, use jsmith@[xxx.xxx.xxx.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. • To use e-mail for paging, use the e-mail address for that recipient’s pager gateway account (for example, `myacct100@skytel.com`). The pager gateway pages the recipient. The recipient’s pager must be able to use text-based messaging.

Setting	Description
SMTP Server	Selects one of the following methods for routing e-mail: • Through the SMTP server provided with the ACPA4000 (the recommended option, **Local**). This option ensures that the e-mail is sent before the 20-second time-out for the ACPA4000, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the SMTP server provided with the ACPA4000 so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the ACPA4000 to forward e-mail to an external mail account. • Directly to the recipient's SMTP server (the **Recipient's** option). On a busy remote SMTP server, the time-out may prevent some e-mail from being sent, and with this option the ACPA4000 tries to send the e-mail only once. When the recipient uses the SMTP server provided with the ACPA4000, the **Recipient's** setting has no effect.
Generation	Enables (by default) or disables sending e-mail to the recipient.
Format	Selects the format used for e-mail messages: **Short**: Identifies only the event that occurred. For example: NetworkAIR ACPA4000: Head Pressure High **Long**: Includes information about the ACPA4000 and the event. For example: Name: TestLab Location: Building 3 Contact: DonAdams http://139.225.6.133 NetworkAIR ACPA4000 Ser #: WS0131005294 Date: 2/25/2004 Time: 16:09:48 Code: 0x1504 Warning - NetworkAIR ACPA4000: Head Pressure High

How to Configure Individual Events

Event List page

The **Actions** option in the **Events** menu opens the **Event Action Configuration** page on the Web interface. Use the **Details** button in this page to access a complete list of the events that can be reported by your Network Management Card.

Note

Modifying events on the **Configure Event Action by Severity Level** page overrides any changes you made to individual events on the **Details** page.

Each event is identified by its unique code, its description, and its assigned severity level. For example:

Code	Description	Severity
0x0002	System: Warmstart	Severe
0x1504	NetworkAIR PA: Head Pressure High	Warning

For information about severity levels and how they define the actions associated with events, see Event Actions (Web Interface Only).

Detailed Event Action Configuration page

The event codes provide a link to a page that allows you to do the following:

- Change the selected event's severity level
- Enable or disable whether the event uses the Event Log, Syslog messages, SNMP traps, or e-mail notifications

Network Menu

Introduction

Overview

The **Network** menu has the options that you use to do the following tasks:

- Define TCP/IP settings, including DHCP or BOOTP server settings, when one of those types of servers is used to provide the required TCP/IP values.
- Use the Ping utility.
- Define and display settings that affect the Network Management Card's settings for DNS, FTP, Telnet, SSH, SNMP, E-mail, Syslog, and the Web interface (SSL).

! **Note**

Only an Administrator has access to the **Network** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- TCP/IP
- DNS
- Send DNS Query (Web interface)
- Ping utility (control console only)
- FTP Server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot mode setting selects the method used to define the three TCP/IP values that a Network Management Card needs to operate on the network:
  - **System IP**: The IP address of the NetworkAIR ACPA4000
  - **Subnet Mask**: The subnet mask value
  - **Default Gateway**: The IP address of the default gateway

See also

For information about how to configure the initial TCP/IP settings using the Management card wizard when you install the NetworkAIR ACPA4000, see the ACPA4000 *Installation, Operation, and Maintenance* manual (**.\doc\en\opmaint.pdf**), provided on the APC NetworkAIR Portable Air Conditioner *Utility* CD and in printed form.

- **Advanced settings** define the Network Management Card's host and domain names, as well as TCP/IP port, BOOTP, and DHCP settings used by the Management Card.

Current TCP/IP settings fields. The current **System IP**, **Subnet Mask**, and **Default Gateway** values, and the Network Management Card's **MAC Address**, **Host Name**, **Domain Name**, and **Ethernet Port Speed** values are displayed above the TCP/IP settings in the control console and the Web interface.

Boot mode setting. This setting selects which method will be used to define the Network Management Card's TCP/IP settings whenever the Network Management Card starts, resets, or restarts:

- **Manual**: Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) that are only available when **Manual** is used to define the needed TCP/IP settings.
- **BOOTP only**: A BOOTP server provides the TCP/IP settings.
- **DHCP only**: A DHCP server provides the TCP/IP settings.
- **DHCP & BOOTP**: The Network Management Card will attempt to get its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server.

Note

An **After IP Assignment** setting will, by default, switch **Boot mode** from its default **DHCP & BOOTP** setting to **BOOTP only** or **DHCP only**, depending on the type of server that supplied the TCP/IP settings to the Network Management Card.

For information about the **After IP Assignment** setting and other settings that affect how the Network Management Card uses BOOTP and DHCP, see Advanced settings. For more information about how to use DHCP, see Boot Mode.

Advanced settings. The **Boot mode** affects which settings are available:

- Two settings are available for all **Boot mode** selections to define the Network Management Card's **Host Name** and **Domain Name** values.
- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).
- Three settings are available for all **Boot mode** selections, except **Manual**, to identify the Network Management Card in BOOTP or DHCP communication:
  - **Vendor Class**: Uses **APC**, by default.
  - **Client ID**: Uses the Network Management Card's MAC address, by default.

    Caution If the **Client ID** is changed from the Network Management Card's MAC address, the new value must be unique on the LAN. Otherwise, the DHCP or BOOTP server may act incorrectly.

  - **User Class**: Uses the Network Management Card's application module type, by default. For example, the NetworkAIR ACPA4000 sets the **User Class** to **NAIRPA**.

- Two settings are available when **BOOTP only** is the Boot mode selection:
  - **Retry Then Fail**: Defines how many times the Network Management Card attempts to discover a BOOTP server before it stops (**4**, by default).
  - **On Retry Failure**: Defines what TCP/IP settings the Network Management Card uses when it fails to discover a BOOTP server (**Use Prior Settings**, by default).

For information about the advanced settings (**DHCP Cookie Is** and **Retry Then Stop**) that directly affect how DHCP is used, see Boot Mode.

DNS

Use these fields to define the IP addresses of the primary and secondary Domain Name Servers (DNS) used by the Network Management Card e-mail feature.

See E-mail Feature and DNS servers.

Send DNS Query (Web interface). Use this option, available only through the **DNS** menu in the Web interface, to send a DNS query that tests the setup of your DNS servers.

Use the following settings to define the parameters for the test DNS request; you view the result of the test DNS request in the **Last Query Response** field (**Passed**, **Failed**, or **Not Responding**).

- Use the **Query Type** setting to select the method to use for the DNS query:
  - The URL name of the server (**Name**)
  - The IP address of the server (**IP**)
  - The Mail Exchange used by the server (**MX**)
- Use the **Query Question** text field to identify the value to be used for the selected **Query Type**:
  - For **Name**, identify the URL.
  - For **IP**, identify the IP address.
  - For **MX**, identify the Mail Exchange address.
- Use the **DNS Server to Query** to select whether to query the primary DNS server or secondary DNS server.

Ping utility (control console only)

Select this option to check the network connection by testing whether a defined IP address responds to the Ping network utility.

By default, the IP address of the default gateway is used. However, you can use the IP address of any device known to be running on the network.

FTP Server

Use the **Access** setting to enable or disable the FTP server. The server is enabled by default.

Note

FTP transfers files without using encryption. For higher security, use Secure CoPy (SCP) for file transfers. When you select and configure Secure SHell (SSH), SCP is enabled automatically. To configure SSH, see Telnet/SSH. If you use SCP for file transfer, disable the FTP server.

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Network Management Card. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5000** to **32767** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port. For example, for a port number of 5000 and a Network Management Card IP address of 159.215.12.114, you would use this command:

```
ftp 159.215.12.114:5000
```

To access a text version of the Network Management Card's event Log, see How to use FTP or SCP to retrieve log files.

See also

To use FTP to download configuration files, see the *Management Card Addendum* (**.\doc\en\addendum.pdf**) on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

Telnet/SSH

Use the **Telnet/SSH** option to perform the following tasks:

- Enable or disable Telnet or the Secure SHell (SSH) protocol for remote control console access.
  - While SSH is enabled, you cannot use Telnet to access the control console.
  - Enabling SSH enables SCP automatically.

    Note

    When SSH is enabled and its port and encryption ciphers configured, no further configuration is required to use SCP. (SCP uses the same configuration as SSH.)

  - Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

  Note

  To use SSH, you must have an SSH client installed. Most Linux and other UNIX® platforms include an SSH client as part of their installation, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

- Configure the port settings for Telnet and SSH.
- Select one or more data encryption algorithms for SSH, version 1; SSH version 2; or both.
- In the Web interface, specify a host key file previously created with the APC Security Wizard and load it to the Network Management Card.

Note

From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file. You must transfer the file to location **/sec** on the Network Management Card.

If you do not specify a host key file, the Network Management Card generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates. **The Network Management Card can take up to 5 minutes to create this host key, and SSH is not accessible during that time.**

- Display the *fingerprint* of the SSH host key for SSH versions 1 and 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or control console of the Network Management Card.

Note

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Network Management Card. Although the delay is not long, it can be mistaken for a problem because there is no explanatory message.

Option	Description
Telnet/SSH Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**. **NOTE:** Enabling SSH automatically disables Telnet. To enable SSH, change the setting and then click **Next>>** in the Web interface or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed.
Protocol Mode	Choose one of the following: • **Telnet:** User names, passwords, and data are transmitted without encryption. • **Secure SHell (SSH), version 1:** User names, passwords, and data are transmitted in encrypted form. There is little or no delay when you are logging on. • **Secure SHell (SSH), version 2:** User names, passwords, and data are transmitted in encrypted form, but with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during data transmission. There is a noticeable delay when you are logging on to the Network Management Card. • **Secure SHell (SSH), versions 1 and 2:** Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

Option	Description
Telnet/SSH Port Configuration	

Telnet Port	Identifies the TCP/IP port used for communications by Telnet with the Network Management Card. The default is **23**.
	You can change the **Port** setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by **User Name** and **Password** settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Network Management Card IP address of 159.215.12.114, your Telnet client would require one or the other of the following commands:
	`telnet 159.215.12.114:5000`
	`telnet 159.215.12.114 5000`

SSH Port	Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Network Management Card. The default is **22**. You can change the **Port** setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by **User Name** and **Password** settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.

Option	Description
SSH Server Configuration	
SSHv1 Encryption Algorithms	Enables or disables **DES**, and displays the status (always enabled) of **Blowfish**, two encryption algorithms (block ciphers) compatible with SSH, version 1, clients. • **DES**: The key length is 56 bits. • **Blowfish**: The key length is 128 bits. You cannot disable this algorithm. **NOTE:** Not all SSH clients can use every algorithm. If your SSH client cannot use **Blowfish**, you must also enable **DES**.
SSHv2 Encryption Algorithms	Enables or disables the following encryption algorithms (Block Ciphers) that are compatible with SSH version 2 clients. • **3DES** (enabled by default): The key length is 168 bits. • **Blowfish** (enabled by default): The key length is 128 bits. • **AES 128**: The key length is 128 bits. • **AES 256**: The key length is 256 bits. **NOTE:** Not all SSH clients can use every algorithm. Your SSH client selects the algorithm that provides the highest security from among the enabled algorithms that it is able to use. (If your SSH client cannot use either of the default algorithms, you must enable an AES algorithm that it can use.)

Option	Description
SSH User Host Key File	
Status:	The **Status** field Indicates the status of the host key (*private* key). In the control console, you display host key status by selecting **Advanced SSH Configuration**. • **SSH Disabled: No host key in use**: No host key has been transferred to the Network Management Card or a host key has been transferred improperly. **NOTE:** A host key must be installed to the **/sec** directory of the Network Management Card. • **Generating**: The Network Management Card is generating a host key because no valid host key was installed in its **/sec** directory. • **Loading**: A host key is being loaded (i.e., being activated on the Network Management Card). • **Valid**: The host key is valid. (If you install an invalid host key, the Network Management Card discards it and generates a valid one. However, a host key that the Network Management Card generates is only 768 bits in length. A valid host key created by the APC Security Wizard is 1024 bits.)
Filename:	You can create a host key file with the APC Security Wizard and then upload it to the Network Management Card by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Network Management Card. **NOTE:** Creating and uploading a host key in advance reduces the time required to enable SSH. If no host key is loaded when you enable SSH, the Network Management Card creates one when it reboots. **The Network Management Card takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.**

Option	Description
SSH Host Key Fingerprint	
SSH v1:	Displays the SSH version 1 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.
SSH v2:	Displays the SSH version 2 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.

SNMP

An **Access** option (the **Settings** option in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.

To define up to four NMSs to serve as trap receivers, see Trap Receiver settings.

<table>
<tr><th>Setting</th><th colspan="2">Definition</th></tr>
<tr><td>Community Name</td><td colspan="2">Defines the password (maximum of 15 characters) that an NMS defined by the <b>NMS IP</b> setting uses to access the channel.</td></tr>
<tr><td>NMS IP</td><td colspan="2">Limits access to the NMS or NMSs specified by the format used for the IP address.
• 159.215.12.1 allows only the NMS with that IP address to have access.
• 159.215.12.255 allows access for any NMS on the 159.215.12 segment.
• 159.215.255.255 allows access for any NMS on the 159.215 segment.
• 159.255.255.255 allows access for any NMS on the 159 segment.
• 0.0.0.0 or 255.255.255.255 allows access for any NMS.</td></tr>
<tr><td rowspan="5">Access Type</td><td colspan="2">Selects how the NMS defined by the NMS IP setting can use the channel when that NMS uses the correct value for <b>Community Name</b>.</td></tr>
<tr><td>Read</td><td>The NMS can use GETs at any time, but it can never use SETs.</td></tr>
<tr><td>Write</td><td>The NMS can use GETs at any time, and can use SETs when no one is logged on to either the control console or Web interface.</td></tr>
<tr><td>Disabled</td><td>The NMS cannot use GETs or SETs.</td></tr>
<tr><td>Write+</td><td>The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface.</td></tr>
</table>

Email

Use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the e-mail feature of the Network Management Card.

See SMTP settings and E-mail Feature.

Syslog

By default, the Network Management Card can send messages to up to four Syslog servers whenever Network Management Card or NetworkAIR PA events occur. The Syslog servers, which must be specifically identified by their IP address, record the events in a log that provides a centralized record of events that occur at network devices.

See also

This user's guide does not describe Syslog, or the Syslog configuration values, in detail. For more information about Syslog, see RFC3164, a copy of which is available at **www.ietf.org/rfc/rfc3164**.

Syslog settings. Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

General Settings	
Setting	**Definition**
Syslog	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code assigned to the Network Management Card's Syslog messages (**User**, by default). **NOTE:** Although other selections are available, **User** is the selection that best defines the Syslog messages sent by a Network Management Card.

Syslog Server Settings	
Server IP	Uses specific IP addresses to identify which of up to four servers will receive Syslog messages sent by the Network Management Card. **NOTE:** To use the Syslog feature, the **Server IP** address must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the Network Management Card will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.

Local Priority (Severity Mapping)	
Map to Syslog's Priorities	Maps each of the severity levels (**Local Priority** settings) that can be assigned to NetworkAIR PA and Network Management Card events to the available Syslog priorities. 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 The following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** • **None** (for events which have no severity level assigned) is mapped to **Info** **NOTE:** To disable sending Syslog messages for **Severe**, **Warning**, or **Informational** events, see Event Actions (Web Interface Only).

Syslog test (Web interface). This option allows you to send a test message to the Syslog servers configured in the **Syslog Server** section.

1. Select the **Priority** to assign to the test message.
2. Define the **Test Message** using any text in the format described in Syslog message format. For example, `NetworkAIR PA: Head Pressure High 0x1504` meets the required message format.
3. Click **Apply** to have the Network Management Card send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

- The priority (PRI) part identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Network Management Card.
- The Header includes a time stamp and the IP address of the Network Management Card.
- The message (MSG) part has two fields:
  - A TAG field, which is followed by a colon and a space, identifies the event type (System or NetworkAIR PA, for example)
  - A CONTENT field provides the event text, followed by a space and the event code

Web/SSL

Use the **Web/SSL** menu to perform the following tasks.

- Enable or disable the two protocols that provide access to the Web interface of the Network Management Card:
  - Hypertext Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission.
  - Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Secure Socket Layer (SSL) encrypts user names, passwords, and data during transmission and provides authentication of the Network Management Card by means of digital certificates.

    See Creating and Installing Digital Certificates to choose among the several methods for using digital certificates.
- Configure the ports that each of the two protocols will use.
- Select the encryption ciphers that SSL will use.
- Identify whether a server certificate is installed on the Network Management Card. If a certificate has been created with the APC Security Wizard but is not installed:
  - In the Web interface, browse to the certificate file and upload it to the Network Management Card.
  - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload it to the location **\sec** on the Network Management Card.

Note

Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Network Management Card creates one when it reboots. **The Network Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

- Display the configured parameters of a digital server certificate, if one is installed.

Option	**Description**
Web/SSL/TLS Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**.
Protocol Mode	Choose one of the following: • **HTTP:** User names, passwords, and data are transmitted without encryption. • **HTTPS (SSL/TLS):** User names, passwords, and data are transmitted in encrypted form, and digital certificates are used for authentication. **NOTE:** To enable **HTTPS (SSL/TLS)**, change the setting and then click **Next>>** in the Web interface, or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen.

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	Identifies the TCP/IP port used for communications by HTTP with the Network Management Card. The default is **80**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Network Management Card IP address of 150.615.12.114, you would use this command: `http://150.615.12.114:5000`
HTTPS Port	Identifies the TCP/IP port used for communications by HTTPS with the Network Management Card. The default is **443**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Network Management Card IP address of 150.615.12.114, you would use this command: `https://150.615.12.114:6502`

Option	Description
SSL/TSL Server Configuration	
CipherSuite	Enables or disables the following SSL encryption ciphers and hash algorithms. (To access these options in the control console, choose **Web/SSL**, then **Advanced SSL/TLS Configuration**.) **NOTE:** All of these encryption ciphers and hash algorithms use the RSA public key algorithm. • **DES (SSL_RSA_WITH_DES_CBC_SHA)**: a block cipher with a key length of 56 bits. The Secure Hash Algorithm (SHA) is used for authentication. • **3DES (SSL_RSA_WITH_3DES_EDE_CBC_SHA)**: a block cipher with a key length of 168 bits. A Secure Hash Algorithm (SHA) is used for authentication. • **RC4 (SSL_RSA_WITH_RC4_128_MD5)**: a stream cipher with a key length of 128 bits, with an RSA key exchange algorithm, and with a Message Digest 5 (MD5) hash algorithm used for authentication. This selection is enabled by default. • **RC4 (SSL_RSA_WITH_RC4_128_SHA)**: a stream cipher with a key length of 128 bits. A Secure Hash Algorithm (SHA) is used for authentication. This selection is enabled by default.

Option	Description
SSL/TLS Server Certificate	
Status:	The **Status** field indicates whether a server certificate is installed. (To display the status in the control console, choose **Web/SSL**, then **Advanced SSL/TLS Configuration**.) • **Not installed**: No certificate is installed on the Network Management Card. **NOTE:** If you install a certificate by using FTP or SCP, you must specify the correct location (**/sec**) on the Network Management Card. • **Generating:** The Network Management Card is generating a certificate because no valid certificate was installed. • **Loading:** A certificate is being loaded (activated on the Network Management Card). • **Valid:** A valid certificate was installed to or generated by the Network Management Card. (If you install an invalid certificate, the Network Management Card discards it and generates a valid one. However, a certificate that the Network Management Card generates has some limitations. See Method 1: Use APC's default certificate.)
Filename:	You can create a server certificate with the APC Security Wizard and then upload it to the Network Management Card by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. By default, the certificate is installed to the correct location. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Network Management Card. However, you must specify the correct location (**/sec**) on the Network Management Card. **NOTE:** Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Network Management Card creates one when it reboots. **The Network Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

Parameter	Description
Current Certificate Details	
Issued to:	**Common Name (CN)**: The IP Address or DNS name of the Network Management Card, except if the server certificate was generated by default by the Network Management Card. For a default server certificate, the **Common Name (CN)** field displays the Network Management Card's serial number. **NOTE:** If an IP address was specified as the Common Name when the certificate was created, use an IP address to log on to the Web interface of the Network Management Card; if the DNS name was specified as the Common Name, use the DNS name to log on. When you log on, if you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue. **Organization (O)**, **Organizational Unit (OU)**, and **Locality, Country:** The name, organizational unit, and location of the organization that is using the server certificate. If the server certificate was generated by default by the Network Management Card, the **Organizational Unit (OU)** field displays "Internally Generated Certificate." **Serial Number:** The serial number of the server certificate.
Issued By:	**Common Name (CN):** The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Network Management Card. For a default server certificate, the Common Name (CN) field displays the Network Management Card's serial number. **Organization (O)** and **Organizational Unit (OU):** The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Network Management Card, the **Organizational Unit (OU)** field displays "**Internally Generated Certificate**."
Validity	**Issued on:** The date and time at which the certificate was issued. **Expires on:** The date and time at which the certificate expires.

Parameter	Description
Fingerprints	Each of the two fingerprints is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser. **SHA1 Fingerprint:** This fingerprint is created by a Secure Hash Algorithm (SHA). **MD5 Fingerprint:** This fingerprint is created by a Message Digest 5 (MD5) algorithm.

System Menu

Introduction

Overview

Use the **System** menu to do the following tasks:

- Configure system identification, date and time settings, and Administrator, Device manager, and Read-Only user access
- Synchronize the real-time clock for the Network Management Card with a Network Time Protocol (NTP) server
- Reset or restart the Network Management Card
- Define the URL links available in the Web interface
- Set the units (Fahrenheit or Celsius) used for temperature displays
- Access hardware and firmware information about the Network Management Card
- Download configuration files (control console only)
- Register for remote monitoring of your ACPA4000

Note: Only an Administrator has access to the **System** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- User Manager
- Identification
- Date & Time
- Tools
- Preferences (Web interface)
- Links (Web interface)
- Remote Monitoring (Web interface)
- About System (Control console)

Note

The **About System** option is a **Help** menu option in the Web interface.

Option Settings

User Manager

Use this option to define the access values shared by the control console and the Web interface, and the authentication used to access the Web interface.

Setting	Definition
Values affecting all users	
Auto Logout	The number of minutes (3 by default) before a user is automatically logged off because of inactivity.
Authentication	The **Basic** setting (default) causes the Web interface to use standard HTTP 1.1 login (base64-encoded passwords); **MD5** causes the Web interface to use an MD5-based authentication login. **NOTE:** Cookies must be enabled at a browser before it can be used with MD5 authentication.
Separate values for Administrator, Device Manager, and Read-only User	
User Name	The case-sensitive name (maximum of 10 characters) used by Administrator and Device Manager users to log on at the control console or Web interface, and by the Read Only User to log on at the Web interface only. • **apc**, by default, for **Administrator** • **device**, by default, for **Device Manager** • **readonly**, by default, for the **Read-only User**
Password	The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but only used to log on to the Web interface when **Basic** is selected for the **Authentication** setting (**apc** is the default **Password** setting for the four account types). **NOTE:** A Read-only user is not permitted to log on through the control console.

Identification

Use this option to define the System **Name**, **Contact**, and **Location** values used by the SNMP agent for the ACPA4000. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

See also

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\mibguide.pdf**) provided on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

Date & Time

Use this option to set the date and time used by the NetworkAIR ACPA4000. The option displays the current settings and allows you to change those settings manually or through a Network Time Protocol (NTP) Server.

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to set **Date** and **Time** for the NetworkAIR ACPA4000.

Note

An **Apply Local Computer Time to System** option, which is available in the Web interface only, sets these values to match the date and time settings of the computer you are using to access the Web interface.

Synchronize with Network Time Protocol (NTP) Server. Use this option on the Web interface, or **Network Time Protocol (NTP)** on the control console, to have an NTP Server automatically update the **Date** and **Time** settings for the NetworkAIR ACPA4000.

Note In the control console, use the **NTP Client** option to enable or disable the NTP Server updates. In the Web interface, use the **Set Manually** option. The updates are disabled by default.

Setting	Definition
Primary NTP Server	Identifies the IP address of the primary NTP server.
Secondary NTP Server	Identifies the IP address of the secondary NTP server when a secondary server is available.
Time Zone	Defines the offset to be used from Greenwich Mean Time (GMT) based on the time zone in which the ACPA4000 is located.
Update Interval	Defines how often, in weeks, the ACPA4000 will access the NTP Server for an update (1 week minimum, 52 weeks maximum). Use **Update Using NTP Now** to initiate an immediate update as well.

Tools

Use this option to restart the Network Management Card or to reset some or all of its configuration settings to their original default values.

Action	**Definition**
No Action (Web Interface only)	No change to the Network Management Card.
Reboot	Restarts the Network Management Card.
Reset to Defaults	Resets all configuration settings. This option will reset the TCP/IP settings and enable DHCP and BOOTP.
Reset to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP settings.
Reset Only TCP/IP to Defaults	Resets the TCP/IP settings only. **NOTE:** With **Boot mode** set to **DHCP & BOOTP**, its default setting, the ACPA4000's TCP/IP settings must be defined by a DHCP or BOOTP server. See TCP/IP.
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the ACPA4000 so that you can reconfigure these components of your security system.
XMODEM (serial connection only)	Allows you to download firmware using a terminal-emulation program when you use a local connection to the control console. To connect to the control console locally, see Local access to the control console.

Preferences (Web interface)

Use this option to define whether temperature values are displayed as **Fahrenheit** or **Celsius** in the Web interface.

Links (Web interface)

Use this option to modify the links to APC Web pages.

Setting	Definition
User Links	
Name	Defines the link names that appear in the **Links** menu (by default, **APC's Web Site**, **Testdrive Demo**, and **Remote Monitoring**).
URL	Defines the URL addresses used by the links. By default, the following URL addresses are used: • **http://www.apc.com** (APC's Web Site) • **http://testdrive.apc.com** (Testdrive Demo) • **http://rms.apc.com** (Remote Monitoring) **NOTE:** Only links of type http:// can be used in these fields. For information about these pages see Links menu.
Access Links	
APC Home Page	Defines the URL address used by the APC logo at the top of all Web interface pages (by default, **http://www.apc.com**).

Remote Monitoring (Web interface)

APC provides fee-based monitoring of your equipment through its Remote Monitoring Service (RMS). If you decide to use RMS, complete the required fields and click **Send RMS Registration**. A confirmation e-mail will provide you with further instructions.

About System (Control console)

This option identifies the following hardware information for the Network Management Card: **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, and **MAC Address**.

This screen also displays **Name**, **Version**, **Date**, and **Time** for the Application Module and AOS.

The **About System** menu also includes fields for system **Flash Type** and the **Type**, **Sector**, and **CRC 16** for each module.

Note

In the Web interface, except for **Flash Type**, this hardware information is reported by the **About System** option in the **Help** menu.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Network Management Card can use a dynamic host configuration protocol (DHCP) server to provide the settings that it needs to operate on a TCP/IP network.

The method that is used to provide the network settings for the Network Management Card depends on **Boot mode**, a **TCP/IP** option in the **Network** menu. To use a DHCP server to provide the network assignment for the Network Management Card, **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.

See also

For more details on DHCP and DHCP options, see RFC2131 and RFC2132, which are available at **www.ietf.org/rfc/rfc2131** and **www.ietf.org/rfc/rfc2132**.

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Network Management Card is started or reset:

1. The Network Management Card makes up to five requests for its network assignment from any BOOTP server. If a valid BOOTP response is received, the Network Management Card starts the network services and sets **Boot mode** to **BOOTP Only**.
2. If the Network Management Card fails to receive a valid BOOTP response after five BOOTP requests, the Network Management Card makes up to five requests for its network assignment from any DHCP server. If a valid DHCP response is received, the Network Management Card starts the network services and sets **Boot mode** to **DHCP Only**.

Note

To configure the Network Management Card so that it always uses the **DHCP & BOOTP** setting for **Boot mode**, enable the **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option, which is disabled by default.

See Network Management Card settings.

3. If the Network Management Card fails to receive a valid DHCP response after five DHCP requests, it repeats BOOTP and DHCP requests until it receives a valid network assignment. First it sends a BOOTP request every 32 seconds for 12 minutes, then it sends one DHCP request with a time-out of 64 seconds, and so forth.

Note

If a DHCP server responds with an invalid offer (e.g., without the APC Cookie), the Network Management Card accepts the lease from that server on the last request of the sequence and immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.

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

DHCP Configuration Settings

Network Management Card settings

The **TCP/IP** option in the **Network** menu of the Web interface and control console accesses the network settings for the Network Management Card.

Three settings (**Port Speed**, **Host Name**, and **Domain Name**) are available regardless of the **TCP/IP** option's **Boot mode** selection, and three settings (**Vendor Class**, **Client ID**, and **User Class**) are available for any **Boot mode** selection except **Manual**.

When **Boot mode** is set to **DHCP & BOOTP**, two options are available:

- **After IP Assignment** in the control console (or **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** in the Web interface): By default, this option switches **Boot mode** to **DHCP Only** or **BOOTP Only**, depending on the configuration of the server that provided the TCP/IP settings.
- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.

For more information about the APC cookie, see DHCP response options.

When **Boot mode** is set to **DHCP Only,** two options are available:

- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.

  For more information about the APC cookie, see DHCP response options

- **Retry Then Stop** in the control console (or **Maximum # of Retries** in the Web interface): This option sets the number of times the Network Management Card will repeat the DHCP request if it does not receive a valid response. By default, the number of retries is 0, which sets the Network Management Card to continue repeating the DHCP request indefinitely.

DHCP response options

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

The Network Management Card uses the Vendor Specific Information option (option 43) in a DHCP response to determine whether the DHCP response is valid.

Vendor Specific Information (option 43). The Vendor Specific Information option contains up to two APC specific options encapsulated in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

APC Cookie. Tag 1, Len 4, Data “1APC”

Option 43 notifies the Network Management Card that a DHCP server has been configured to service APC devices. By default, the APC Cookie must be present in this DHCP response option before the Network Management Card can accept the lease.

Note Use the **DHCP Cookie Is** setting described in Network Management Card settings to disable the APC cookie requirement.

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
```

Boot Mode Transition. Tag 2, Len 1, Data 1/2

This option 43 setting enables or disables the **After IP Assignment** option which, by default, causes the **Boot mode** option to use the setting that reflects the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**):

- For a data value of 1, the **After IP Assignment** option is disabled, and the **Boot mode** option remains in its **DHCP & BOOTP** setting after successful network assignment. Whenever the Network Management Card restarts, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.

See DHCP & BOOTP boot process.

- For a data value of 2, the **After IP Assignment** option is enabled and the **Boot mode** option switches to **DHCP Only** when the Network Management Card accepts the DHCP response. Whenever the Network Management Card restarts, it will request its network assignment (TCP/IP settings) from a DHCP server only.

For more information about the **After IP Assignment**, see Network Management Card settings.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. The Network Management Card uses the following options within a valid DHCP response to define its TCP/IP settings:

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

Miscellaneous options. The Network Management Card uses the following options within a valid DHCP response to define NTP, DNS, hostname, and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): Identifies up to two NTP servers that can be used by the Network Management Card.
- **NTP Time Offset** (option 2): Specifies the offset, in seconds, of the subnet for the Network Management Card from Coordinated Universal Time (UTC).
- **DNS Server, Primary and Secondary** (option 6): Identifies one or two DNS servers that can be used by the Network Management Card.
- **Host Name** (option 12): Identifies the hostname (maximum length of 32 characters) to be used by the Network Management Card.
- **Domain Name** (option 15): Identifies the domain name (maximum length of 64 characters) to be used by the Network Management Card.

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the NetworkAIR ACPA4000 is subject to the same exposure as other devices on the network.

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

Summary of access methods

Serial control console.

Security Access	Description
Access is by user name and password.	Always enabled.

Remote control console.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure SHell (SSH)	For high security, use SSH. • With Telnet, the user name and password are transmitted as plain text. • SSH disables Telnet and provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission.

SNMP.

Security Access	Description
Available methods: • Community Name • NMS IP filters • Agent Enable/Disable • 4 access communities with read/write/disable capability	The NMS IP filters allow access from designated IP addresses. • 162.245.12.1 allows only the NMS with that IP address to have access. • 162.245.12.255 allows access for any NMS on the 162.245.12 segment. • 162.245.255.255 allows access for any NMS on the 162.245 segment. • 162.255.255.255 allows access for any NMS on the 162 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.

File transfer protocols.

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

Web Server.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • MD5 authentication • Secure Socket Layer (SSL) and Transport Layer Security (TLS)	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase. SSL and TLS are available on Web browsers supported for the NetworkAIR ACPA4000 and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the ACPA4000, immediately change the default user names and passwords. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP, or Web/SSL/TLS server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra “password,” hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard “well known ports” for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

User names, passwords, community names (SNMP)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the control console or Web interface of the NetworkAIR ACPA4000. If your network requires the higher security of the encryption-based options available for the control console and Web interface, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Authentication

Authentication versus encryption

You can select to use security features for the NetworkAIR ACPA4000 that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

For a security method that provides additional authentication for the Web interface, but does not provide the higher security of encryption, use Message Digest 5 (MD5) Authentication.

See MD5 authentication (for the Web interface).

To ensure that data and communication between the NetworkAIR ACPA4000 and the client interfaces, such as the control console and the Web interface, cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. You can also use these protocols in combination with MD5 authentication.
- To encrypt user names and passwords for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure CoPy (SCP) protocol.

For more information on these protocols for encryption-based security, see Secure SHell (SSH) and Secure CoPy (SCP) and Secure Socket Layer (SSL)/Transport Layer Security (TLS).

MD5 authentication (for the Web interface)

The Web interface option for MD5 authentication enables a higher level of access security than the basic HTTP authentication scheme. The MD5 scheme is similar to CHAP and PAP remote access protocols. Enabling MD5 implements the following security features:

- The Web server requests a user name and a password phrase (distinct from the password). The user name and password phrase are not transmitted over the network, as they are in basic authentication. Instead, a Java login applet combines the user name, password phrase, and a unique session challenge number to calculate an MD5 hash number. Only the hash number is returned to the server to verify that the user has the correct login information; MD5 authentication does not reveal the login information.
- In addition to the login authentication, each form post for configuration or control operations is authenticated with a unique challenge and hash response.
- After the authentication login, subsequent page access is restricted by IP addresses and a hidden session cookie. (You must have cookies enabled in your browser.) Pages are transmitted in their plain-text form, with no encryption.

If you use MD5 authentication for the Web interface, be sure to increase the security for other interfaces to the ACPA4000.

- **Control console:** Use SSH (which disables Telnet) for encrypted access.
- **File transfer:** Disable FTP, and instead use SCP, which encrypts user names, passwords, and files.
- **SNMP:** Disable SNMP or disable its write access. With read-only access, trap facilities remain available.

See also

For additional information on MD5 authentication, see RFC document #1321 at **http://www.ietf.org**, the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

You can use MD5 and the encryption-based SSL/TSL security protocols together. See Secure Socket Layer (SSL)/ Transport Layer Security (TLS) for an example of the extra security benefits of using both.

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the NetworkAIR ACPA4000) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the NetworkAIR ACPA4000) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.

See also

To create a host key, see the *Management Card Addendum* (**.\doc\en\addendu7m.pdf**) on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

- The NetworkAIR ACPA4000 supports versions 1 and 2 of SSH. The encryption mechanisms of the versions differ, and each version has advantages. Version 1 provides faster login to the Network Management Card, and version 2 provides improved protection from attempts to intercept, forge or change data that are transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.

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

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

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is **not** disabled by enabling SSH.

Secure Socket Layer (SSL)/Transport Layer Security (TLS)

For secure Web communication, you enable Secure Socket Layer (SSL) and Transport Layer Security (TLS) by selecting HTTPS (SSL/TLS) as the protocol mode to use for access to the Web interface of the NetworkAIR ACPA4000. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the web server to the user. Originally developed by Netscape, it has become an internet standard supported by most Web browsers.

The NetworkAIR ACPA4000 supports SSL version 3.0 and TLS version 1.0. Most browsers let you select the version of SSL to enable.

When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen.

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the NetworkAIR ACPA4000). The browser verifies the following:

- The format of the server certificate is correct.
- The server certificate's expiration date and time has not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority.

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the APC Security Wizard, provided on the APC NetworkAIR Portable Air Conditioner *Utility* CD, to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Network Management Card.

See Creating and Installing Digital Certificates for a summary of how these certificates are used.

See also

To create certificates and certificate requests, see the Network Management Card *Addendum* (**.\doc\en\addendum.pdf**) on the APC NetworkAIR Portable Air Conditioner *Utility* CD.

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data (i.e. that it has not been intercepted and sent by another server).

See CipherSuite to select which authentication and encryption algorithms to use.

You can use SSL/TLS and MD5 authentication together to provide the security benefits of both. MD5 authentication does not provide encryption, but its authentication methods can be a useful enhancement to the security provided by SSL/TLS.

Note

Web browsers cache (save) Web pages that you recently accessed and allow you to return to those pages without re-entering your user name and password. MD5 authentication, however, requires you to enter your user name and password even to access a cached Web page, e.g., when you use the **Back** button of Microsoft Internet Explorer.

Therefore, if you use the SSL and TLS protocols without also using MD5 authentication, always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the NetworkAIR ACPA4000 supports the use of digital certificates with the Secure Socket Layer (SSL) protocol. Digital certificates can authenticate the NetworkAIR ACPA4000 (the server) to the Web browser (the SSL client).

The sections that follow summarize the three methods of creating, implementing, and using digital certificates. Read these sections to determine the most appropriate method for your system.

- Method 1: Use APC's default certificate.
- Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate.
- Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.

Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Choosing a method for your system

Using the Secure Socket Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use APC's default certificate. When you enable SSL, you must reboot the Network Management Card. During rebooting, if no server certificate exists on the Network Management Card, the Network Management Card generates a default server certificate that is signed by APC but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**
  - Before they are transmitted, the user name and password for Network Management Card access and all data to and from the Network Management Card are encrypted.
  - You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.
- **Disadvantages:**
  - The Network Management Card takes up to 5 minutes to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
  - This method does not include the browser-based authentication provided by a CA certificate (a certificate signed by a Certificate Authority) as Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, whenever you log on to the Network Management Card, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available and asking if you want to proceed.

– The default server certificate on the Network Management Card has the Network Management Card's serial number in place of a valid *common name* (the DNS name or the IP address of the Network Management Card). Therefore, although the Network Management Card can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read Only User**), the browser cannot authenticate what Network Management Card is sending or receiving data.

– The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate. You use the APC Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the APC Security Wizard uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Network Management Card.
- A *server certificate* that you upload to the Network Management Card. When the APC Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Network Management Card sending or requesting data:

- To identify the Network Management Card, the browser uses the *common name* (IP address or DNS name of the Management Card) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a “trusted” signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Network Management Card access and all data to and from the Network Management Card are encrypted.
  - The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than

the public key used in Method 1. (This longer encryption key is also used in Method 3.)

– The server certificate that you upload to the Network Management Card enables SSL to authenticate that data are being received from and sent to the correct Network Management Card. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.

– The root certificate that you install to the browser enables the browser to authenticate the Network Management Card's server certificate to provide additional protection from unauthorized access.

- **Disadvantage:**

  Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser. See Method 3.)

Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. You use the APC Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the APC Security Wizard to create a server certificate (a **.p15** file) that includes the signature from the root certificate returned by the Certificate Authority. You upload the server certificate to the Network Management Card.

Note You can also use Method 3 if your company or agency operates its own Certificate Authority, Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Network Management Card access and all data to and from the Network Management Card are encrypted.
  - You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Network Management Card.
  - The length of the *public key* (RSA key) that is used for setting up an SSL session is 1024 bits, providing more complex encryption and

consequently a higher level of security than the public key used in Method 1 (This longer encryption key is also used in Method 2.)

- The server certificate that you upload to the Network Management Card enables SSL to authenticate that data are being received from and sent to the correct Network Management Card. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The browser matches the digital signature on the server certificate that you uploaded to the Network Management Card with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.

- **Disadvantages:**
  - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
  - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

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

Product Information

Warranty Statement

LIMITED PRODUCT WARRANTY FOR APC PRODUCTS

The limited warranty provided by American Power Conversion Corporation ("APC") in this Statement of Limited Factory Warranty applies only to Products you purchase for your commercial or industrial use in the ordinary course of your business.

LIMITED FACTORY WARRANTY

APC product covered

NetworkAIR PA Portable Air Conditioning Unit

Terms of warranty

APC warrants that the Product shall be free from defects in materials and workmanship for a period of one (1) year from the date of start-up when APC authorized service personnel performed the start-up of the Product, or a maximum of 18 months from the date of Product shipment from APC, when APC authorized service personnel have not performed the start-up of the Product ("Warranty Period"). In the event that the Product fails to meet the foregoing warranty, APC shall repair or replace any defective parts, such repair or replacement to be without charge for on-site labor and travel if APC authorized personnel have conducted start-up of the Product. An APC Start-Up Service must be performed/completed by APC authorized service personnel or replacement of defective parts only will be covered. APC shall have no liability and no obligation to repair the installed Product if non-authorized personnel performed the start-up and such start-up caused the Product to be defective. Any parts furnished under this warranty may be new or factory-remanufactured. **This warranty does not cover** circuit breaker resetting, loss of refrigerant, consumables, or preventative maintenance items. **Repair or replacement of a defective product or part thereof does not extend the original warranty period.**

Non-transferable Warranty extends to first purchaser for use

This Warranty is extended to the first person, firm, association or corporation (herein referred to by “You or Your”) for whom the APC Product specified herein has been purchased. This Warranty is not transferable or assignable without the prior written permission of APC.

Assignment of warranties

APC will assign to you any warranties which are made by manufacturers and suppliers of components of the APC Product and which are assignable. Any such warranties are assigned “AS IS” and APC makes **no representations** as to the effectiveness or extent of such warranties, assumes NO RESPONSIBILITY for any matters which may be warranted by such manufacturers or suppliers and extends no coverage under this Warranty to such components.

Drawings, descriptions

APC warrants for the Warranty Period and on the terms of the Warranty set forth herein that the APC Product will substantially conform to the descriptions contained in the APC Official Published Specifications or any of the drawings certified and agreed to by an authorized APC representative, if applicable thereto ("Specifications"). It is understood that the Specifications are **not warranties of performance** and **not warranties of fitness for a particular purpose**.

Warranty claims procedure

To obtain service under Warranty, contact APC Customer Support at (800) 800-4272. You will need the model number of the Product, the serial number, and the date purchased. A technician will ask you to describe the problem. If it is determined that the Product will need to be returned to APC you must obtain a returned material authorization (RMA) number from APC Customer Support. Products that must be returned must have the RMA number marked on the outside of the package, and be returned with transportation charges prepaid. If it is determined by APC Customer Support that on-site repair of the Product is allowed, APC will arrange to have APC authorized service personnel dispatched to the Product location to repair or replace the Product at the discretion of APC.

Exclusions

APC shall not be liable under the Warranty if its testing and examination discloses that the alleged defect in the product does not exist or was caused by your or any third person's misuse, negligence, improper installation or testing, unauthorized attempts to repair or modify, or any other cause beyond the range of the intended use, or by accident, fire, lightning or other hazard.

THERE ARE NO WARRANTIES, EXPRESSED OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, OF PRODUCTS SOLD, SERVICED OR FURNISHED UNDER THIS AGREEMENT OR IN CONNECTION HEREWITH. APC DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTION AND FITNESS FOR A PARTICULAR PURPOSE. THE APC EXPRESS WARRANTIES WILL NOT BE ENLARGED, DIMINISHED, OR AFFECTED BY AND NO OBLIGATION OR LIABILITY WILL ARISE OUT OF APC RENDERING TECHNICAL OR OTHER ADVICE OR SERVICE IN CONNECTION WITH THE PRODUCTS. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES. THE WARRANTIES SET FORTH ABOVE, CONSTITUTE SOLE LIABILITY OF APC AND YOUR EXCLUSIVE REMEDY FOR ANY BREACH OF SUCH WARRANTIES. THE WARRANTIES EXTEND ONLY TO YOU AND ARE NOT EXTENDED TO ANY THIRD PARTIES.

IN NO EVENT SHALL APC, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES BE LIABLE FOR ANY FORM OR INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING OUT OF THE USE, SERVICE OR INSTALLATION OF THE PRODUCTS, WHETHER SUCH DAMAGES ARISE IN CONTRACT OR TORT, IRRESPECTIVE OF FAULT, NEGLIGENCE OR STRICT LIABILITY OR WHETHER APC HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGE.

Warranty Procedures

Labor

- APC will support labor costs if a quality issue is found during start-up that is determined to be caused by workmanship or a factory defect.
- The mechanical contractor who is performing the repairs must call APC technical services to obtain a repair authorization number before any work is started.
- The mechanical contractor must provide detailed information, (photos, start-up sheets) to APC technical services before any repairs are started.
- If any repairs are performed without prior authorization, APC will not pay for any labor cost.
- APC will not support claims for any of the following:
  - Truck rental
  - Travel time
  - Rental on recovery machine and cylinders
  - Gas mileage
  - Solder, flux, sil-phos, silver solder, and silver solder flux.
- APC will pay for $2.50 per pound for refrigerant.

To obtain a repair authorization number for a NetworkAIR product, call APC NetworkAIR technical services between 8:00 A.M. and 5:00 P.M. Eastern time, Monday through Friday:

- Phone: (1)(888)695-6500 (USA and Canada, toll free)
- Fax: (1)(401)788-2691

Parts

- APC warrants the parts of their systems for 1 year from the date of start-up or 18 months from the shipping date of the system. This warranty covers only the cost of the part and not the labor for installation.
- Warranty parts requests need to have specific unit information (serial number, model number, job number) to allow proper identification and processing of the warranty part transaction.
- A purchase order may be required to issue any warranty part. An invoice will be sent once a parts order is filled and shipped to the field. You have 30 days to return a part to APC. After 30 days, the warranty invoice will be outstanding and payment of the invoice will be expected in full.
- Return authorization documentation will be sent with any replacement part. This documentation must be sent back with the defective part to APC for proper identification of the warranty return. Mark the warranty return number on the outside of the package.
- After the part has been received at APC, APC will determine the status of the credit based on an examination of the returned part. Parts that are damaged from: lack of maintenance, mis-application, improper installation, shipping damage, and acts of man/nature will not be covered under the parts warranty.
- For any warranty parts request received before 1:00 PM EST, the part will be shipped Same Day Standard Ground delivery. Any costs

associated with Next Day or Airfreight will be the responsibility of the party requesting the part.

- Shipping costs for warranty parts are the responsibility of the sender.

To request warranty parts, contact APC NetworkAIR division technical services.

Phone: (1)(888)695-6500 (USA and Canada, toll-free)

Fax: (1)(401)788-2691

Recycling the Battery

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

Life-Support Policy

General policy

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

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

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

Examples of life-support devices

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

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

Index

APC Worldwide Customer Support

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

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

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

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

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

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

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

Copyright

990-1702 **02/2004**

CERTIFIED
InfraStruXure
by APC