USER'S GUIDE

MasterSwitch Plus

Contents

Introduction

Product Description

Features of MasterSwitch Plus

MasterSwitch Plus allows you to individually control power to connected equipment and to gracefully shut down or restart up to eight connected servers running different operating systems. In order to manage your system effectively and efficiently, MasterSwitch Plus has these additional features:

- Four password-protected accounts that ensure restricted access to system-, device-, read-only- and outlet-level services.
- Automatic shut-down of connected servers attached to an APC UPS when the UPS enters an on-battery state and removes power from connected equipment after the server confirms shutdown.
- Shuts down servers before cycling power to the connected equipment (Graceful Reboot).
- Control of eight power outlets (per unit) for complete and flexible management of connected equipment.
- Web, control console, or SNMP management interfaces.
- Configure the sequence in which outlets receive power upon start-up.
- Connects serially to up to three expansion units (AP9225EXP), providing control of 32 connected devices with one IP address.
- Provides a selection of security protocols for authentication and encryption.
- Event log accessible by FTP, SCP, Telnet, serial connection, or a Web browser.

Note

The MasterSwitch Plus does not provide power protection. Therefore, APC does not recommend plugging a unit directly into any unprotected power source, such as a wall outlet.

Initial setup

You must define three TCP/IP settings for the MasterSwitch Plus before it can operate on the network.

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

To configure the TCP/IP settings, see the MasterSwitch Plus *Installation and Quick Start Manual*, provided on the APC MasterSwitch *Utility* CD and on the APC Web site (www.apc.com).

Access Procedures

Overview

The MasterSwitch Plus has two internal interfaces (control console and Web interface) that provide menus with options that allow you to manage the unit. The SNMP interface also allows you to use an SNMP browser with the PowerNet® Management Information Base (MIB) to manage the unit.

For more information about the internal user interfaces, see Control Console and Web Interface.

To use the PowerNet MIB with an SNMP browser, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide*, provided on the APC MasterSwitch *Utility* CD and on the APC Web site (www.apc.com).

Access priority for logging on

Only one user at a time can log on to the unit 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 unit always has the highest priority.
- Telnet or Secure SHell access to the control console from a remote computer has priority over Web access.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.

Types of user accounts

The MasterSwitch Plus has three levels of access (Administrator, Device Manager, and Outlet User), all of which are protected by password and user name 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 use only the following menus (the default user name is **device** and the password is **apc**):
  - the Device Manager menu and its sub-menus in the control console, and all menus in the top section of the navigation panel of the Web interface (MasterSwitch Plus and **Outlets**)
  - the Log option in the **Events** menu in the Web interface (a Device Manager can also access the event log in the control console by pressing `Ctrl-L`.)
- 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, delete data, or use FTP-related options. Links to configuration options are visible but disabled, and the event and data logs display no **Delete** button.

  The Read-Only User's default **User Name** is **readonly**, and the default **Password** is **apc**.
- An Outlet User can access only the following menus:
  - the **Control** option of the **Outlets** menu on the web interface
  - the Device Manager menu and the **Outlet Control** sub-menus in the control console

To set the Administrator, Device Manager, or Outlet User user name and password settings, see User Manager or Outlet Usr Mgt.

How to Recover From a Lost Password

You can use a local computer, a computer that connects to the Management Card 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 serial cable (940-0024 or 940-1524) to the selected port on the computer and to the configuration port at the Management Card.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port as follows:
   - 9600 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER as many times as necessary to redisplay 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 redisplayed, 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 a complete description of how to download a firmware upgrade for your MasterSwitch Plus, see File Transfers.

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

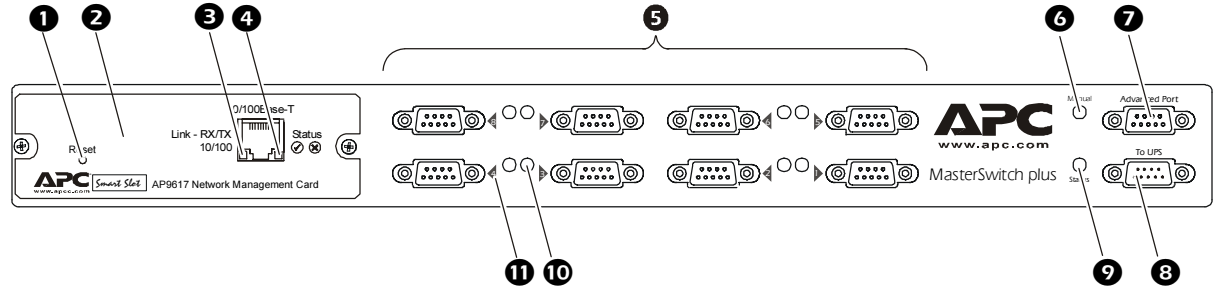
1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied smart-signaling cable (940-0024) to connect the selected port to the serial port on the front panel of the unit.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter your user name and password (both **apc**, for administrators only) and press the Enter key.
6. From the **Control Console** menu, select **System**, then **Tools**, then File Transfer, then **XMODEM**.
7. At the prompt `Perform transfer with XMODEM-CRC?` type `yes`, and press ENTER.
8. The system will then prompt you to choose a transfer rate and to change your terminal settings to match the transfer rate. Press ENTER to set the MasterSwitch Plus to accept the download.
9. In the terminal program, send the file using the XMODEM protocol. Upon completion of the transfer, the console will prompt you to restore the baud rate to normal.

Do not interrupt the upgrade.

The MasterSwitch Plus will restart when the download is complete.

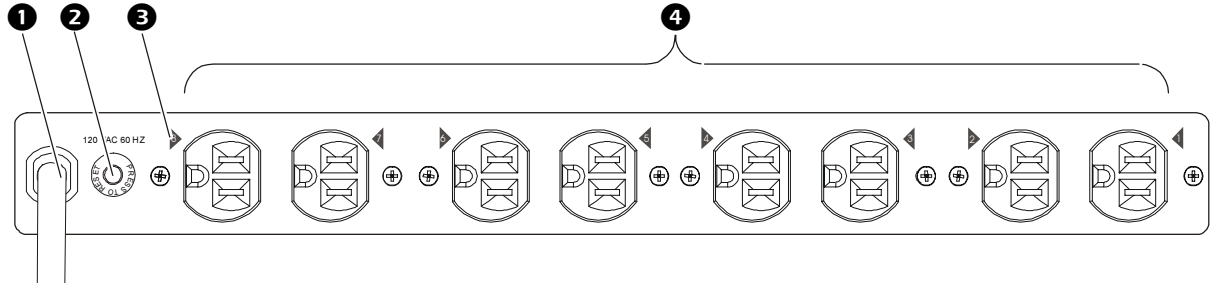
Upgrading the firmware will not interfere with the operation of the outlets.

Front Panel



	Item	Function
❶	Reset Button	Resets the MasterSwitch Plus without affecting the outlet status.
❷	Network Management Card	Allows you to use a Web browser, Telnet, or a serial interface to remotely manage the MasterSwitch Plus and connected devices (AP9225 only).
❸	Status LED	See Status LED.
❹	Link RX/TX LED	See Link-RX/TX (10/100) LED.
❺	Basic Ports	Connects the MasterSwitch Plus to servers running PowerChute or built-in UPS monitoring software.
❻	Manual Button	Issues a Battery Capacity Override command or cancels a Master Power On Delay, depending on the situation. See Manual button for details.
❼	Advanced Port	Allows the connected server to communicate with a UPS operating in Advanced Signaling Mode and can also be used as a management port.
❽	To UPS Port	Connects the MasterSwitch Plus to a UPS or another unit with the supplied cable (APC part number 940-1000).
❾	MasterSwitch Plus Status	See MasterSwitch Plus Status LED.
❿	Basic Port LED	See Basic Port LED
⓫	Port Label	Corresponds to the outlet number on the rear panel.

Rear Panel



	Item	Function
1	Power Cord	Provides input power to the MasterSwitch Plus (120 VAC 60 HZ).
2	Circuit Breaker	Press the button to reset the circuit breaker.
3	Outlet Label	Relates each outlet to its corresponding basic port.
4	Outlets	Eight controllable outlets that provide power to connected equipment.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	One or more of the following situations exist: • The Management Card is not receiving input power. • The cable that connects the Management Card to the network is disconnected or defective. • The device that connects the Management Card to the network is turned off or not operating correctly. • The Management Card itself is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid Green	The MasterSwitch Plus is connected to a network operating at 10 Mbps.
Solid Orange	The MasterSwitch Plus is connected to a network operating at 100 Mbps.
Flashing Green	The MasterSwitch Plus is receiving or transmitting data packets from the network at 10 Mbps.
Flashing Orange	The MasterSwitch Plus is receiving or transmitting data packets from the network at 100 Mbps.

Status LED

This LED indicates the network status of the MasterSwitch Plus.

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

1 If you do not use a BOOTP or DHCP server, see the MasterSwitch Plus *Installation and Quick Start Manual,* provided on the APC MasterSwitch *Utility* CD and on the APC Web site (www.apc.com) to configure the TCP/IP settings.
2 To use a DHCP server, see Boot Mode.

Basic Port LED

LED State	Definition
On	The outlet is on.
Off	The outlet is off.
Mostly off[1]	The outlet is off with a pending action to turn on.
Mostly on[2]	The outlet is on with a pending action to turn off.
Flashing green	The outlet cannot turn on due to an environmental alarm.

1 The LED flashes on and off, with the off state lasting longer.
2 The LED flashes off and on, with the on state lasting longer.

MasterSwitch Plus Status LED

LED State	Definition
Off	MasterSwitch Plus has no power.
Solid green	MasterSwitch Plus has valid network settings.
Flashing green	MasterSwitch Plus does not have valid network settings. See the Installation Manual for more information.
Flashing red slowly	MasterSwitch Plus is making a BOOTP request.
Solid red	MasterSwitch Plus has detected a hardware failure.

Manual button

The manual button is used to cancel two different commands. If this button is pressed for at least 1/2 second and then released, one of the following results will occur:

- If the MasterSwitch Plus is waiting for the Master Power On Delay to expire, MasterSwitch Plus issues a cancel command. The diagram in Unit/Outlet start-up sequence illustrates the outlet's behavior when the Master Power On Delay is cancelled.
- If the configuration contains a UPS and the UPS is operating on AC power, MasterSwitch Plus issues a Battery Capacity Override command. The diagram in Unit/Outlet start-up sequence illustrates the outlet's behavior when the Battery Capacity Override command is issued.

If neither of the above conditions is true, pressing the manual button has no effect.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the unit 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 unit implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the unit 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 reboots itself.

Resetting the network timer

To ensure that the unit does not reboot if the network is quiet for 9.5 minutes, the unit attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the unit, 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 unit from rebooting.

MasterSwitch Plus Properties

Outlet properties

Outlet properties are governed by two operating modes: Annunciator and Graceful Shutdown. Some outlet properties are common to both control modes, while other properties are specific to an operating mode.

Property	Control Mode	Default Setting for Outlet Modes							
		1	2	3	4	5	6	7	8
Outlet Control Mode	N/A	Graceful Shutdown Mode							
Name: Outlet #___	Both	1	2	3	4	5	6	7	8
Power On Time Delay (seconds)	Graceful Shutdown	0	2	4	6	8	10	12	14
Battery Capacity Threshold	Graceful Shutdown	0%							
Low Battery Warning Control (minutes)	Graceful Shutdown	4.5							
Power Off Time Delay (seconds)	Graceful Shutdown	120							
UPS Low Battery Multiplier	Graceful Shutdown	1							
Will Device Confirm	Graceful Shutdown	No							
Restart Delay	Graceful Shutdown	Remain Off							
Reboot Duration (seconds)	Graceful Shutdown	5							
Initial State (non-alarm)	Annunciator	Off							
Alarm Action Delay (seconds)	Both	15							
Environment Alarm Masks	Both	Disabled (for each Environment alarm)							

MasterSwitch Plus configuration

Configuration of MasterSwitch Plus is dependent upon your application. You can use only “on-demand” operations (On, Off, Shutdown, and Reboot), or you can couple on-demand operations with “unattended” shutdown features.

To use only on-demand operations, see Configuring an outlet for on-demand operation. To use the “unattended” shutdown features of MasterSwitch Plus in addition to the on-demand operations, see Configuring an outlet for unattended shutdown.

MasterSwitch Plus behaviors

The diagrams, starting with Unit/Outlet start-up sequence, define the behaviors for every event recognized by the MasterSwitch Plus unit. You customize the unit‘s behavior by choosing specific values for the unit and outlet properties. All outlet and unit properties on the diagrams are highlighted hotlinks that lead you to the property’s definition. All outlet and unit properties are defined in MasterSwitch Plus Menus.

Configuring an outlet for on-demand operation

Configuring an outlet for on-demand operation requires selecting values for the following properties:

Property	Used in Sequence Diagram
Unit Properties	
Power On Time Delay	Unit/Outlet start-up sequence
Outlet Properties	
Outlet Control Mode	No diagram available

Property	Used in Sequence Diagram
Reboot Duration	Reboot sequence and Graceful reboot sequence
Device Confirm	Graceful shutdown sequence, Graceful shutdown sequence for On-battery events, Graceful shutdown sequence for environment alarms, and Graceful reboot sequence
Power Off Delay	Graceful shutdown sequence, Graceful shutdown sequence for On-battery events, Graceful shutdown sequence for environment alarms, and Graceful reboot sequence
Restart Delay	Graceful shutdown sequence
Power On Delay	Unit/Outlet start-up sequence, Graceful shutdown sequence, Graceful shutdown sequence for On-battery events, Graceful shutdown sequence for environment alarms, and Delayed On sequence

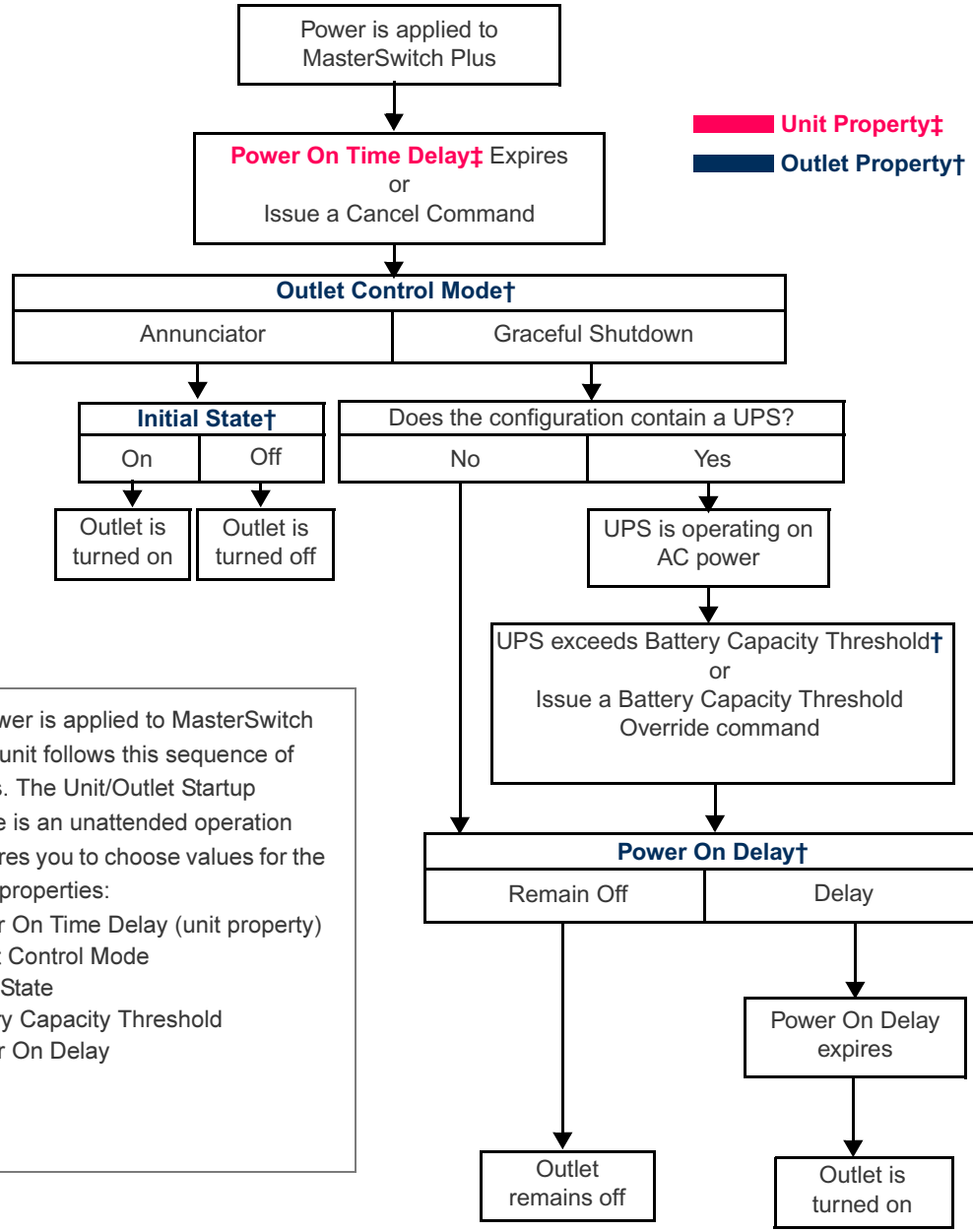
Configuring an outlet for unattended shutdown

Configuring an outlet for unattended shutdown requires selecting values for the following properties:

Property	Used in Sequence Diagram
Unit Properties	
Power On Time Delay	Unit/Outlet start-up sequence
Outlet Properties	
Graceful Shutdown	
UPS Low Battery Multiplier	Graceful shutdown sequence for On-battery events
Low Battery Warning Control	Graceful shutdown sequence for On-battery events

Property	Used in Sequence Diagram
Device Confirm	Graceful shutdown sequence, Graceful shutdown sequence for On-battery events, Graceful shutdown sequence for environment alarms, and Graceful reboot sequence
Power Off Delay	Graceful shutdown sequence for On-battery events, Graceful shutdown sequence for environment alarms, and Graceful reboot sequence
Annunciator	
Alarm Action Delay	Graceful shutdown sequence for environment alarms and Annunciator sequence for environment alarms

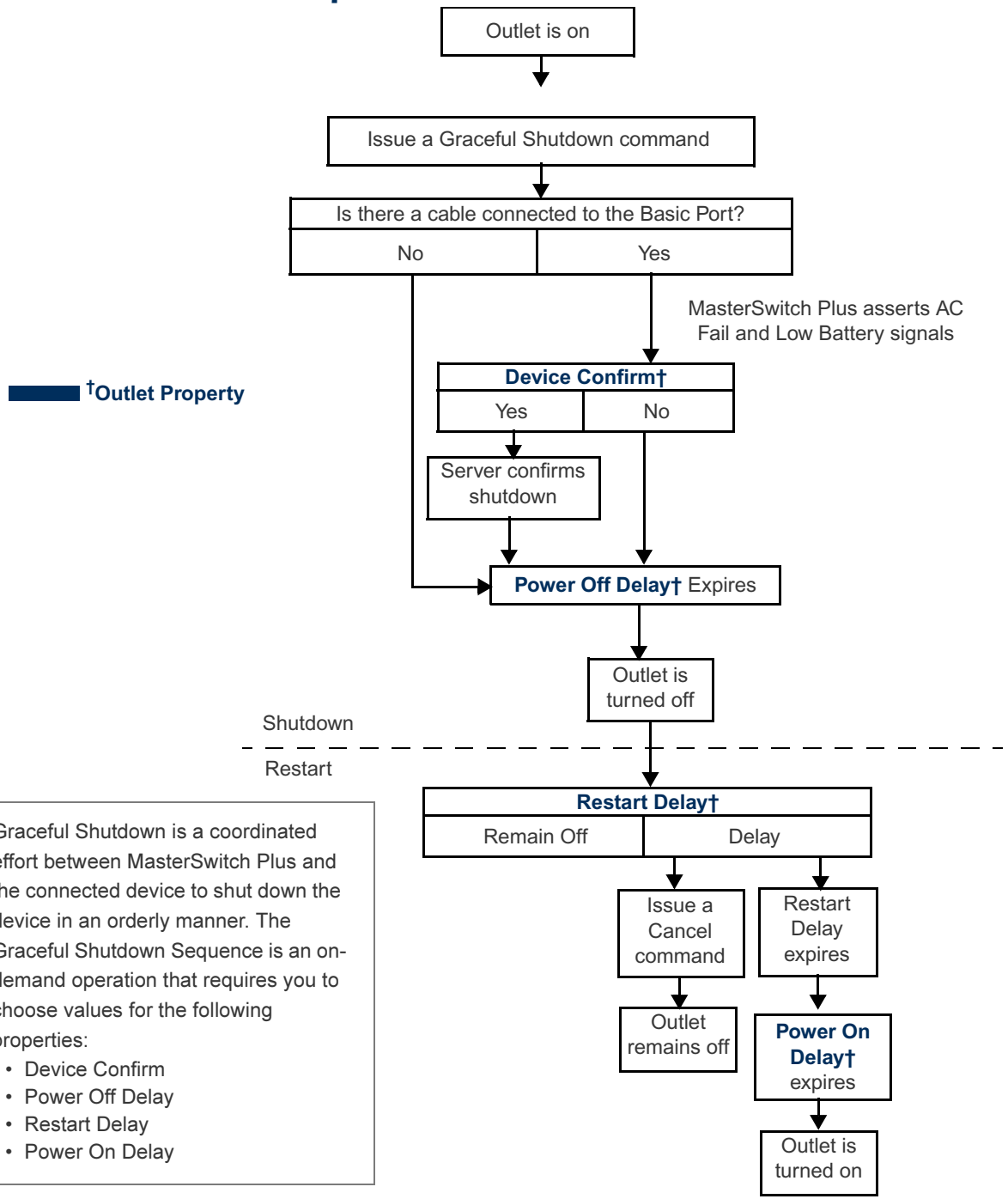
Unit/Outlet start-up sequence



When power is applied to MasterSwitch Plus, the unit follows this sequence of behaviors. The Unit/Outlet Startup Sequence is an unattended operation that requires you to choose values for the following properties:

- Power On Time Delay (unit property)
- Outlet Control Mode
- Initial State
- Battery Capacity Threshold
- Power On Delay

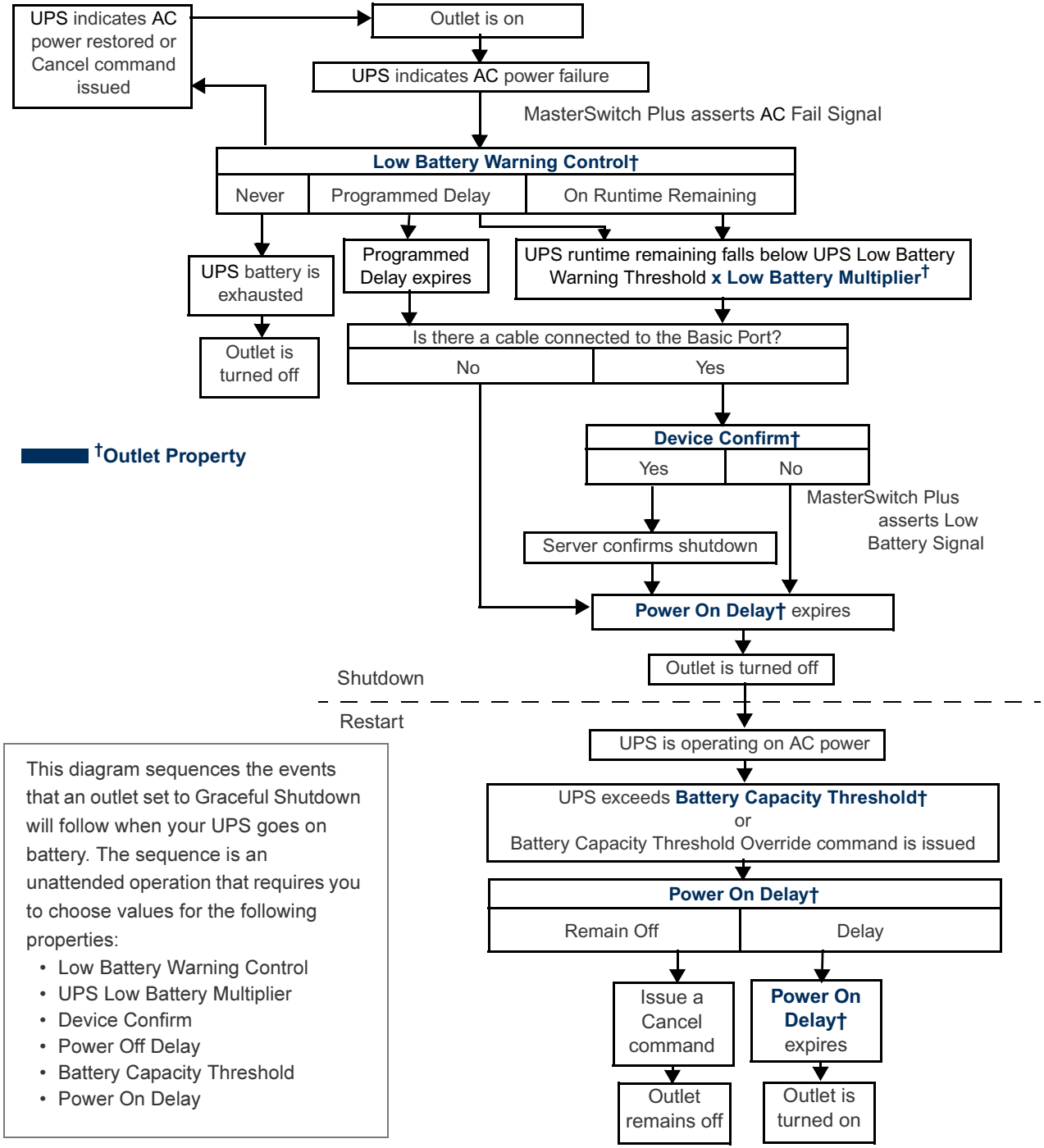
Graceful shutdown sequence



Graceful Shutdown is a coordinated effort between MasterSwitch Plus and the connected device to shut down the device in an orderly manner. The Graceful Shutdown Sequence is an on-demand operation that requires you to choose values for the following properties:

- Device Confirm
- Power Off Delay
- Restart Delay
- Power On Delay

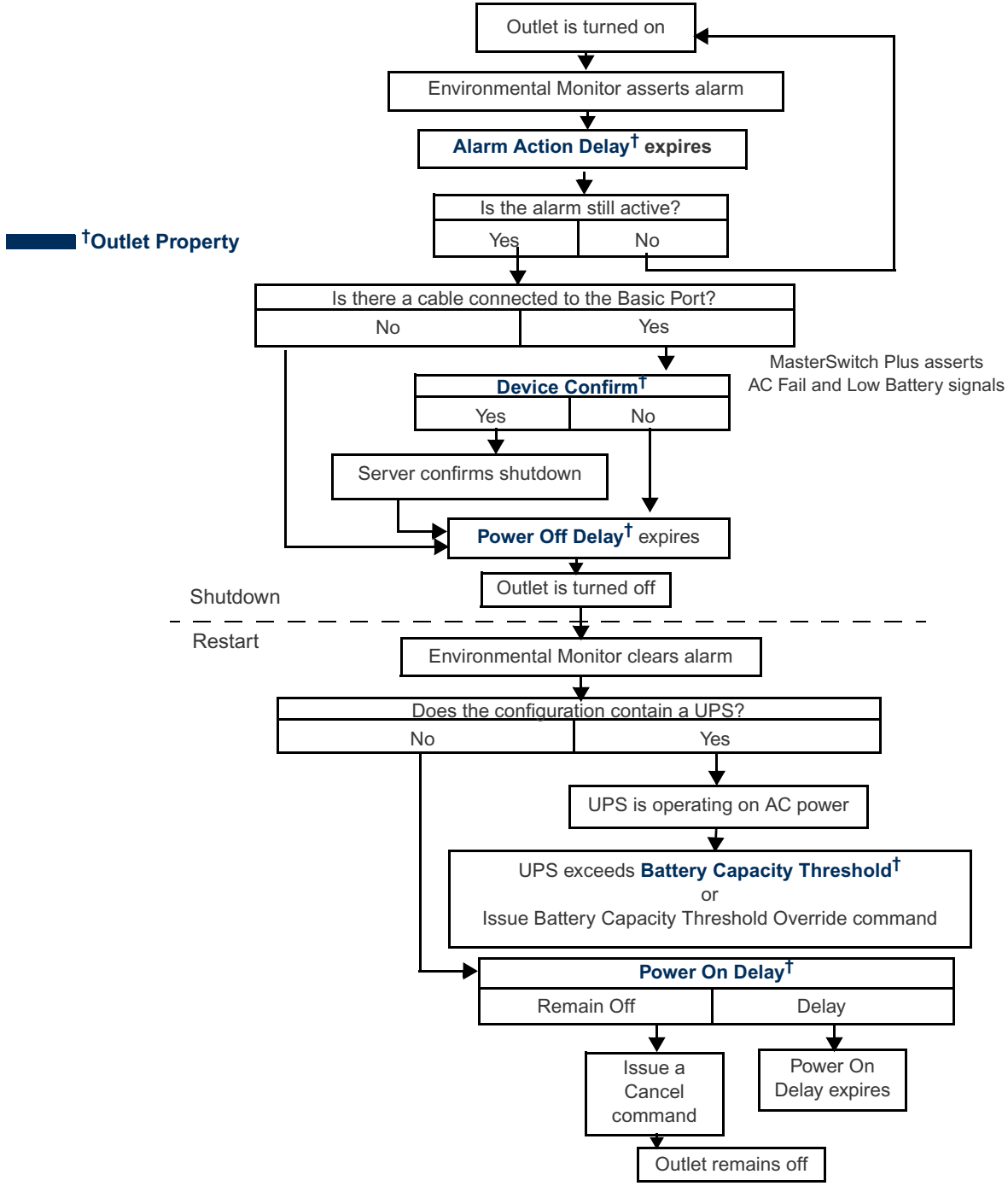
Graceful shutdown sequence for On-battery events



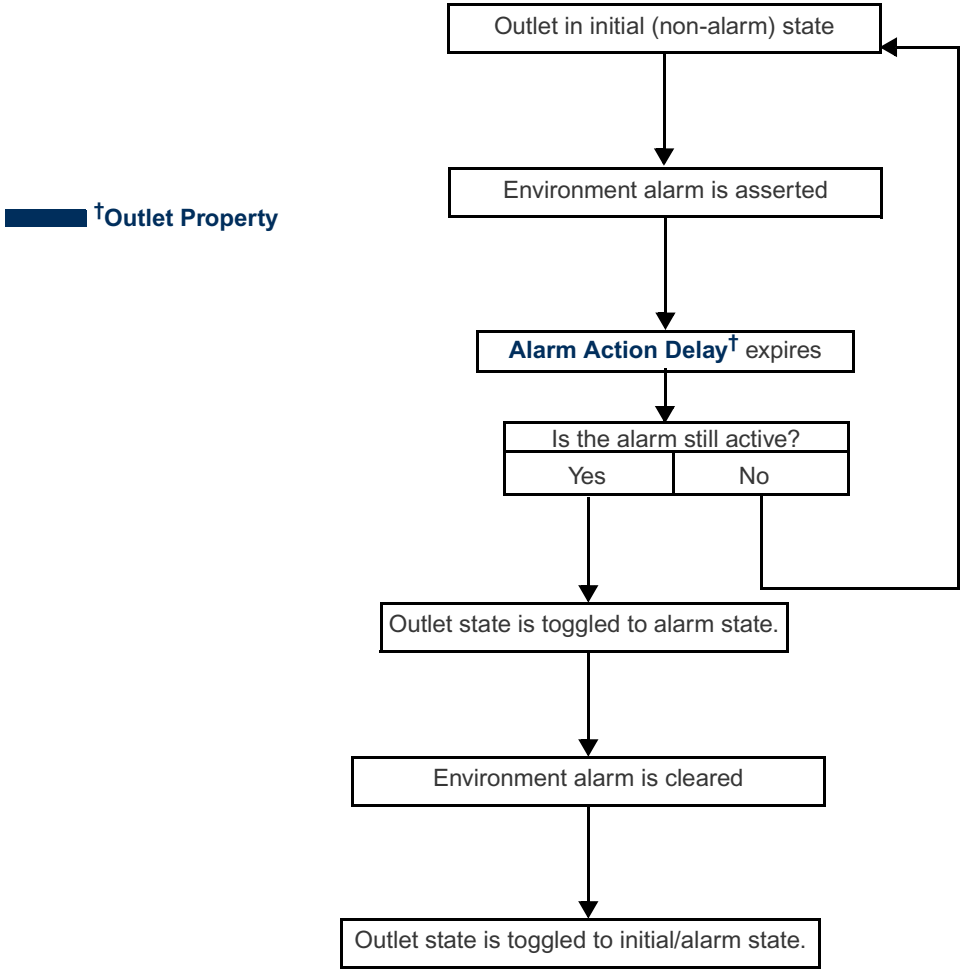
This diagram sequences the events that an outlet set to Graceful Shutdown will follow when your UPS goes on battery. The sequence is an unattended operation that requires you to choose values for the following properties:

- Low Battery Warning Control
- UPS Low Battery Multiplier
- Device Confirm
- Power Off Delay
- Battery Capacity Threshold
- Power On Delay

Graceful shutdown sequence for environment alarms

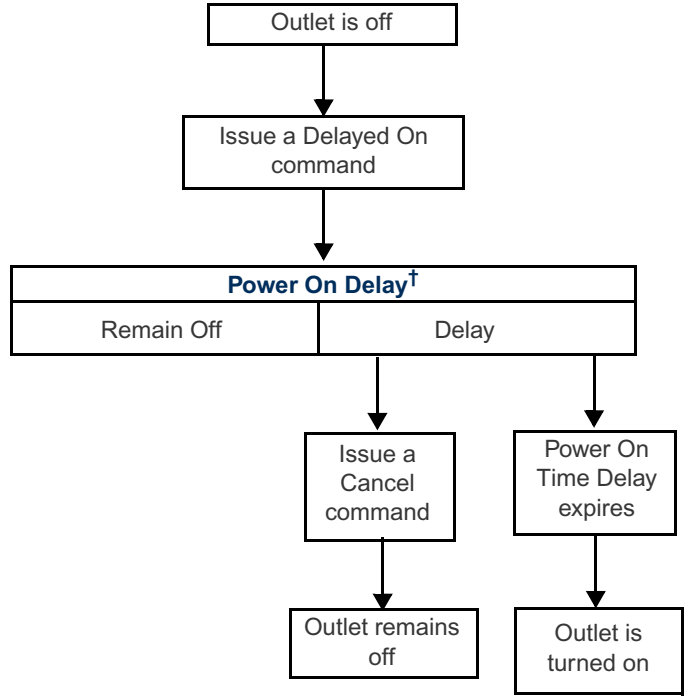


Annunciator sequence for environment alarms



This diagram sequences the events that an outlet set to Annunciator will follow when your Environmental Monitor issues an alarm. The sequence is an unattended operation that requires you to choose a value for the Alarm Action Delay property.

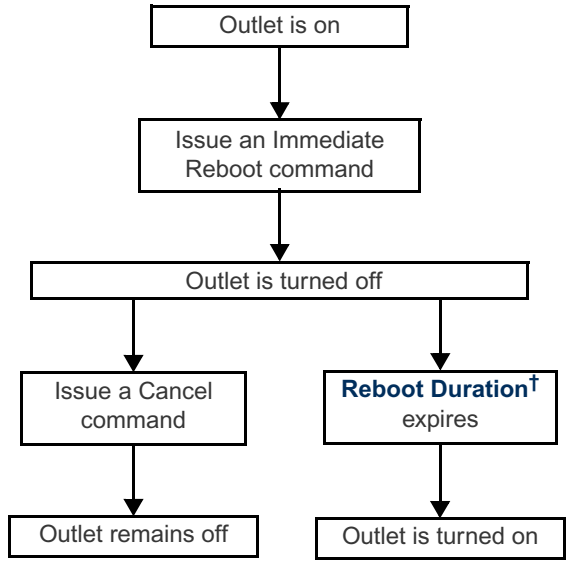
Delayed On sequence



†Outlet Property

This diagram sequences the events that an outlet will follow when you issue a Delayed On command. The sequence is an on-demand operation that requires you to choose a value for the Power On Delay property.

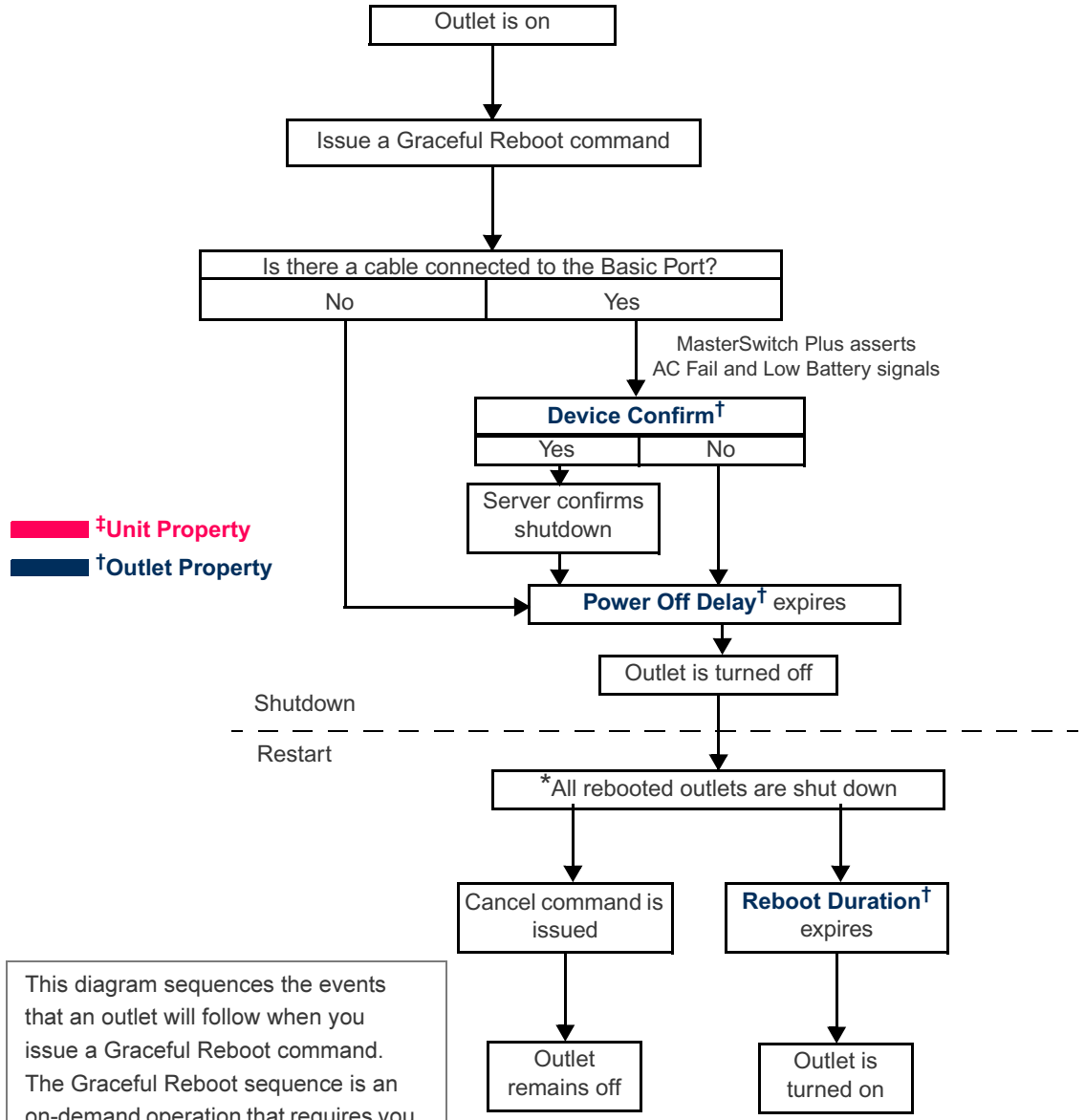
Reboot sequence



†Outlet Property

This diagram sequences the events that an outlet will follow when you issue an Immediate Reboot command. The sequence is an on-demand operation that requires you to choose a value for the Reboot Duration property.

Graceful reboot sequence



This diagram sequences the events that an outlet will follow when you issue a Graceful Reboot command. The Graceful Reboot sequence is an on-demand operation that requires you to choose values for the following properties:

- Will Device Confirm?
- Power Off Delay
- Reboot Duration

* If this command is applied to all outlets, the Reboot Duration delay for an outlet will not begin until all the outlets have shut down.

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 Management Card (when the Management Card uses the default Telnet port of 23), and press ENTER. For example:

   ```
   telnet 139.225.6.133
   ```

Note

If the Management Card uses a non-default port number (between 5000 and 32768), you need to include a colon or a space (depending on your Telnet client) between the IP address and 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 unit through the serial port on the front 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 (940-0024) to connect the selected port to the serial port on the front panel of the unit.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.

Main Screen

Example main screen

The main screen that is displayed when you log on to the control console of a unit.

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


American Power Conversion              Network Management Card AOS v2.6.4
(c) Copyright 2004 All Rights Reserved  MSP  APP                    v2.6.2
-------------------------------------------------------------------------------
Name      : MS Plus Rack 14                          Date : 02/22/2005
Contact   : Bill Cooper                              Time : 10:16:58
Location  : Data Center                              User : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes                Stat : P+ N+ A+

MS plus 1: Serial Communication Established (MS Plus)

------- 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 uses a name that identifies the type of device that connects to the network. In the Example main screen, the application firmware for the unit is displayed.

```
Network Management Card AOS   v2.6.4
MSP APP                       v2.6.2
```

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

```
Name      : MS Plus Rack 14
Contact   : Bill Cooper
Location  : Data Center
```

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

- The **Up Time** field reports how long the unit has been running since it was last reset or since power was applied.

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

- Two fields identify when you logged on, by **Date** and **Time**.

```
Date : 02/22/2005
Time : 10:16:58
```

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

```
User : Administrator
```

Main screen status fields.

- The **Stat** field reports the unit 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 unit failed to connect to the network.
N !	Another device is using the IP address of the unit.
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.

If the AOS status is not P+, contact APC Worldwide Customer Support, even if you can still access the unit.

- The unit model and name field reports the status of the unit. For example:

```
MasterSwitch Plus: Serial 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 corresponding 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 (Administrator and Device Manager only)

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
```

When you log on as Device Manager or as an Outlet User, you will not have access to the **System** or **Network** menus.

Device Manager option

This option accesses the **Device Manager** menu. Select the units you want to manage from this menu. Each connected MasterSwitch Plus is available from this menu.:

```
1- MasterSwitch plus 1
2- MasterSwitch plus 2
```

Network option

Use this option to do the following tasks:

- Configure the TCP/IP settings for the unit
- Use the Ping utility
- Define settings that affect the FTP, Telnet, Web interface and SSL, SNMP, e-mail, DNS, and Syslog features of the MasterSwitch Plus

System option

Use this option to do the following tasks:

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

Web Interface

How to Log On

Overview

You can use the DNS name or System IP address of the unit 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 three account types.

There is no default password for Outlet user accounts. (An administrator must define the password and other account characteristics for an Outlet user.)

See Outlet Usr Mgt.

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, and an IP address was spcified as the common name in the certificate, you must use an IP address to log on to the Management Card. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

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

Supported Web browsers

As your browser, you can use the Microsoft® Internet Explorer (IE) browser (5.0 and higher) or the Netscape® browser (7.0 and higher) to access the unit 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 the data log require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Rack PDU 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 Rack PDU.
- Configure the proxy server so that it does not proxy the specific IP address of the Rack PDU.

In addition, the unit 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 unit.
- Configure the proxy server so that it does not proxy the specific IP address of the unit.

URL address formats

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.

If the error "You are not authorized to view this page" occurs (Internet Explorer only), someone is logged onto 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 Internet Explorer, you must type http:// or https:// as part of the address when any port other than 80 is used.).

For more information, see FTP server, Telnet/SSH, and 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 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 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

When you log on to the Web interface at the MasterSwitch Plus, 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:

- MasterSwitch Plus **Status** shows the status of each connected MasterSwitch Plus, MasterSwitch Plus expansion unit, and Environmental Monitoring Unit.
- **Outlet Status** shows outlet, outlet name, and outlet state.
- **Environment** shows threshold violations and the state of contact alarms.
- **10/100 Management Card Status** shows the following:
  - **Name**, **Contact,** and **Location** information for the MasterSwitch Plus.
  - Date and time the screen was last refreshed.
  - **User** (**Administrator**, **Device Manager**, **Read Only User**, or **Outlet User**) type.
  - How long (**Up Time**) the MasterSwitch Plus has been running since it was last started or reset.

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.

Navigation Menu

Overview

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

- IP address of the unit
- MasterSwitch Plus menus to manage the unit and its components
  - **Outlets**
  - MasterSwitch Plus menu (for each attached unit)
- Menus to manage the event log, data log, network connection, and system parameters
  - **Events**
  - **Data**
  - **Network**
  - **System**

When you log on as a Device Manager, the **Network** and **System** menus do not appear in the navigation menu.

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

Select a menu to perform a task

To do the following, see the Outlets Menu:

- Control power to any of the individual AC outlets on the rear panel of the unit.
- Control power to all of the AC outlets on the rear panel of the unit.
- Schedule **daily**, **weekly**, or **one-time** outlet events.

To do the following, see the MasterSwitch Plus Menus:

- Set the device name.
- Enable or disable the manual button on the front of the MasterSwitch Plus.
- Set the **Power On Time Delay**.
- Set outlet names, modes, and links.
- Enable and disable environmental alarm actions.

To do the following, see Environment Menu:

- Display the sensor status, input contact, and output relay status.
- Configure external sensor parameters and input contact settings.

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 Data Menu (Web Interface Only):

- Access the data log.
- Define the log interval (how often data will be sampled and recorded) for the data log.

To do the following, see Network Menu:

- Configure new **TCP/IP** settings for the unit.
- Identify the Domain Name System (**DNS**) Server, test its network connection, and enable or disable DNS Reverse Lookup Event Logging (which logs the domain name of the device associated with each event).
- Define settings that affect FTP, Telnet and SSH, the Web interface and SSL, SNMP, Syslog, and e-mail.

To do the following, see System Menu:

- Control **Administrator**, **Device Manager**, and **Read Only User** access.
- Control **Outlet User** access.
- Configure **RADIUS** parameters.
- Define the system **Name**, **Contact**, and **Location** values.
- Set the date and time used by the unit.
- Through the Tools menu:
  - Restart the MasterSwitch Plus.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates
  - Upload a user configuration file.
- Select **Fahrenheit** or **Celsius** for temperature displays.
- Define the URL addresses of the user links and APC logo links in the Web interface, as described in Links menu.

Help menu

When you click **Help**, the **Contents** page 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 information about the unit's **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 were created.

In the control console, the **About System** option, in the **System** menu, identifies the **Flash Type** used.

Links menu

This 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.
4. Click **Apply**.

The link associated with the APC logo is also definable.

MasterSwitch Plus Menus

Outlets Menu

Control

Web interface. To control all of the outlets at once, select a **Control Action** under the **Master** heading and click **Apply**.

To control individual outlets, select a **Control Action** for each outlet under the individual outlet's heading, and click **Apply**.

Control console. To control all outlets at once, select the MasterSwitch Plus unit you want to control from the **Device Manager** menu, and select option 9 — **ALL Outlets**. Select **Outlet Control** and a control action. Type YES and press ENTER to execute the change.

To control outlets individually, select the MasterSwitch Plus unit you want to control from the **Device Manager** menu, and select the outlet you want to control. Select **Outlet Control** and choose a control action from the list. Type YES and press ENTER to execute the change.

Action Name	Description	Available Modes
Immediate On	Immediately turns an outlet on. This command is available anytime after the unit's Power On Time Delay has expired and the outlet is off. (Available in both Annunciator and Graceful Shutdown modes.)	Annunciator Graceful Shutdown
Sequenced On	Apply power to the outlet according to its Power On Delay Time. Only available for master control of outlets in graceful shutdown mode.	Graceful Shutdown Only

Action Name	Description	Available Modes
Delayed On	Apply power to the outlet after its Power On Delay expires. Only available in graceful shutdown mode.	Graceful Shutdown Only
Immediate Off	Immediately removes power from an outlet.	Annunciator Graceful Shutdown
Graceful Reboot	Removes and then reapplies power to an outlet. If the connected server is running shutdown software, such as PowerChute Network Shutdown, and is connected to MasterSwitch Plus with the appropriate signaling cable, this operation will ensure that your server's operating system is shut down before power is removed from the outlet. If the server is not connected to the MasterSwitch Plus, then MasterSwitch Plus will remove power from the outlet after the Power Off Time Delay expires. Power is reapplied after the Reboot duration expires. If this command is applied to all outlets, the Reboot Duration delay for an outlet will not begin until all the outlets have shut down.	Graceful Shutdown Only
Immediate Reboot	Immediately removes power from an outlet and reapplies power after the outlet's Reboot Duration expires.	Graceful Shutdown Only

Action Name	Description	Available Modes
Shutdown	Removes power and then optionally reapplies power to an outlet. If the connected server is running shutdown software, such as PowerChute Network Shutdown, and is connected to MasterSwitch Plus with the appropriate signaling cable, this operation will ensure that your server's operating system is shut down before power is removed from the outlet. If the server is not connected to the MasterSwitch Plus, MasterSwitch Plus will remove power from the outlet after the Power Off Time Delay expires. Specify a Restart delay to reapply power automatically.	Graceful Shutdown Only
Override	If the UPS battery charge has not exceeded the Battery Capacity Threshold, selecting the override action will allow power to be applied to an outlet.	Graceful Shutdown Only
Cancel	Cancel a delayed startup or shutdown.	Graceful Shutdown Only

Configure Outlets

Web interface. Click the outlet number link (for example 1:3) and make changes to **Outlet Name**, **Outlet Mode**, and **Outlet Links**. Click **Apply** to accept the changes.

Control console. To configure outlets individually, select the MasterSwitch Plus unit you want to control from the **Device Manager** menu, and select the outlet you want to configure. Select **Outlet Configuration** and choose a configuration setting from the list. Select **Accept Changes** to apply the new settings.

Setting	Description
Outlet Name	Identifies each outlet.
Outlet Control Mode	Establishes mode for associated outlet. All on-demand operations are available when the Outlet Control mode is set to Graceful Shutdown. When set to Annunciator, only Immediate On and Immediate Off operations are available.
Outlet Link (Web only)	The outlet's HTTP or HTTPS link in URL form.
Will Device Confirm	Indicates whether the device connected to the outlet can assert a shutdown signal.
Low Battery Warning Control	Selects the method MasterSwitch Plus uses for determining when to assert the outlet's Low Battery signal after the UPS has switched to battery operation.
UPS Low Battery Multiplier	A low battery signal is generated when the UPS's remaining battery runtime falls below this value multiplied by the UPS Low Battery Warning.
Restart Delay	The delay between removing power from an outlet due to a Graceful Shutdown and reapplying power to that outlet.
Power Off Delay	The time from the triggering event (such as a server confirming a shutdown) until power is removed from the outlet.

Setting	Description
Power On Delay	Determines the time interval between the triggering event and power being applied to the outlet.
Reboot Duration	The delay between removing power from an outlet because of a reboot and reapplying power to an outlet.
Alarm Action Delay	The amount of time that an Environment alarm must be asserted before the unit reacts to the alarm.
Battery Capacity Threshold	Sets the minimum percentage of Battery Capacity required of the UPS before power can be applied to an outlet.

Scheduling

To schedule an outlet event, select **Scheduling**. Select **daily**, **weekly**, or **one-time** under the **Summary** heading. Enter your information and click **Apply**.

MasterSwitch + Menu

Device Config (Outlet Config in Control Console)

Web interface. To set the name of the device, to set the **Power On Delay** for the outlets for this device, and to disable or enable the Manual button on the front of the MasterSwitch Plus, select the MasterSwitch **+** menu, change the setting you wish to modify, and click **Apply**.

Control console. To set the name of the device, to set the **Power On Delay** for the outlets for this device, and to disable or enable the Manual button on the front of the MasterSwitch Plus, select the **Device Manager** menu. Select the MasterSwitch Plus or expansion unit you want to modify and then select **ALL Outlets**. Select **Outlet Configuration**. Change the **Name/Location**, **Manual Button**, and **Power On Time Delay** fields, and then select **Accept Changes** to apply the new settings.

Setting	Description
Name	Set the name for this MasterSwitch Plus unit.
Manual Button	Activate or deactivate the Manual button on the front panel of the unit.
Power On Time Delay	Set how long the MasterSwitch Plus will delay after AC power is applied, before starting the outlet's power-on sequence.
Restore Factory Defaults (control console only)	Resets the original settings for the MasterSwitch Plus unit. All unit and outlet properties are set to their defaults.
View Manufacturing Data	Displays the following information: Model Number, Manufacture Date, Hardware Rev, Firmware Rev, and Serial Number. The Web interface displays this data under the **Help** menu.

Setting	Description
View Self Test Results (control console only)	Allows you to display the results of the unit's last power-on self-test. The tests performed are: **Program Memory**: Confirms that the EPROM chip is working properly. **Non-Volatile Memory**: Confirms that the EEPROM chip is working properly.

Configure Environmental Alarms

Web interface. Click the **Outlet Config** menu under the MasterSwitch Plus unit you want to configure. Select the Environmental alarms to enable or disable by selecting the check-boxes under each **Enable/Disable Environment Alarm Actions** heading:

- **Zones 1–4**
- **Probe 1**
- **Probe 2**

Click the **Apply** button under each heading to accept the changes.

The Environmental alarms apply only if you have an Environmental Monitoring Card installed in an expansion unit, or if the MasterSwitch Plus is connected to an Environmental Monitoring Unit.

Control console. Select the MasterSwitch Plus unit you want to configure from the **Device Manager** menu, and select the outlet you want to configure. Select **Environmental Alarms Configuration** and choose a configuration setting from the list. Select **Accept Changes** to apply the new settings.

Setting	Definition
Zone 1	Controls the Zone 1 environmental alarm.
Zone 2	Controls the Zone 2 environmental alarm.
Zone 3	Controls the Zone 3 environmental alarm.
Zone 4	Controls the Zone 4 environmental alarm.
Probe 1 Humidity Low Limit	Controls the humidity low limit alarm for the first temperature and humidity sensor.
Probe 1 Humidity High Limit	Controls the humidity high limit alarm for the first temperature and humidity sensor.
Probe 1 Temp Low Limit	Controls the temperature low limit alarm for the first temperature and humidity sensor.
Probe 1 Temp High Limit	Controls the temperature high limit alarm for the first temperature and humidity sensor.
Probe 2 Humidity Low Limit	Controls the humidity low limit alarm for the second temperature and humidity sensor.
Probe 2 Humidity High Limit	Controls the humidity high limit alarm for the second temperature and humidity sensor.
Probe 2 Temp Low Limit	Controls the temperature low limit alarm for the second temperature and humidity sensor.
Probe 2 Temp High Limit	Controls the temperature high limit alarm for the second temperature and humidity sensor.

Environment Menu

Status

Web interface. To view the sensor status for external Environmental Monitor (EM) sensors 1 and 2, input contact and output relay status, and information about the Environmental Monitor, select **Status** from the **Environment** menu.

Control console.

- To view the sensor status for external EM sensors 1 and 2, select **Environment** from the **Device Manager** menu, and select **External Environmental Monitor Settings**.
- To view the input contact and output relay status, select **Contact Settings** from the **External Environmental Monitor Settings** menu.
- To view information about the Environmental Monitor, select **About Environmental Monitor** from the **External Environmental Monitor Settings** menu.

Probes

Web interface. To configure the settings for external EM sensors 1 and 2, select **Probes** from the **Environment** menu, enter your settings and click **Apply**.

Control console. Select:

```
Device Manager > Environment > External Environmental
Monitor Settings > Probe Settings
```

Select the sensor you want to configure. Choose a configuration setting from the list. Select **Accept Changes** to apply the new settings.

Input Contacts

Web interface. To configure the settings for external EM input contacts, select **Input Contacts** from the **Environment** menu, enter your settings and click **Apply**.

Control console. Select:

```
Device Manager > Environment > External Environmental
Monitor Settings > Contact Settings
```

Select the contact you want to configure. Select **Accept Changes** to apply the new settings.

Managing the Expansion Unit

Introduction

Overview

If you have purchased only the MasterSwitch Plus Expansion Unit (AP9225 EXP) without purchasing a MasterSwitch Plus (AP9225), you can configure the Expansion Unit through the serial port using MasterSwitch Plus local control console menus.

Local access to the control console

You can use a local computer that connects to the unit through the serial port on the front 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 (940-0024) to connect the selected port to the serial port on the front panel of the unit.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER to access the internal menus.

When logging on, you will not need a user name.

Navigating the internal interface

The MasterSwitch Plus menus allow you to manage the MasterSwitch Plus expansion unit and an Environmental Monitoring Card. All menus list items by number and name.

- To enter a selection on any of the menus, type its related one- or two-character command and press ENTER.
- To see the results of the last changes you have made, it may be necessary to press ENTER.
- To return to the previous screen, press ESC.
- To exit the MasterSwitch Plus internal menus, type Q (case-sensitive) at the main menu.

Main Menu

Item	Description
Version	Displays the version of the MasterSwitch Plus firmware.
Unit Name	Identifies the MasterSwitch Plus unit that has been accessed. **NOTE:** The Unit Name can be changed in the **Unit Properties** menu.
UPS State	Displays the status of the UPS. The possible states are: • **Inactive** — UPS is in sleep mode. • **On Line** — UPS is operating normally. • **AC Fail** — UPS is operating on battery. • **Unknown** — Communication with UPS has failed.
Outlet Name	Identifies each outlet. **NOTE:** Each outlet's name is changeable at the associated **outlet properties** menu.
Outlet State	Displays the current state of the outlet. The possible states are: • **On** — Outlet is turned on. • **On in hh:mm:ss** — Outlet will be turned on after the specified time period elapses. • **Off** — Outlet is turned off. • **Off in hh:mm:ss** — Outlet will be turned off after the specified time period elapses.
To Change Unit Properties	Instructs you to enter a U to access the **Unit Properties** menu. **NOTE:** The **Enable/Disable Alarms** setting on the **Outlet Properties** menus controls the behavior of an individual outlet with regard to Environment alarms.
To Change Outlet Properties	Instructs you to enter the associated outlet number (1– 8) to access its outlet properties.

Item	Description
To Change Environmental Monitoring Card Properties	Instructs you to enter M to access the Environmental Monitoring Card properties menu (available only if an Environmental Monitoring Card is present).
To Change Units	Instructs you to enter a I to access the next MasterSwitch Plus unit in the cascading setup.
To Change Outlet States	Instructs you to enter various commands to initiate on-demand outlet actions. After entering a command, you will be asked to enter an outlet number (1– 8) to perform the action on the associated outlet or you will be asked to enter an A to perform the action on all of the outlets. The commands you may enter are: • **N** — On: Immediately turns an outlet on. • **TS** — Shutdown: Gracefully shuts down and optionally restarts an outlet. • **C** — Cancel: Cancels a delayed startup or shutdown. • **D** — Delayed On: Turns an outlet on after the outlet's Turn On Delay expires. • **F** — Off: Immediately turns an outlet off. • **R** — Reboot: Immediately turns an outlet off and turns it back on after the outlet's Reboot Duration expires. • **Y** — Graceful Reboot: Gracefully shuts down and restarts an outlet. • **O** — Override: Allows an outlet to restart when the UPS battery charge has not exceeded the Battery Capacity Threshold.

Unit Properties Menu

Item	Description
Name	Set the name of this MasterSwitch Plus unit. A maximum of 23 printable ASCII characters is allowed.
Address	Specify the unit's address (1– 4) in a cascading setup. Enter 1 for the unit connected closest to the UPS, 2 for the unit adjacent to unit 1, and so on for up to four units. See the *Installation and Quick-Start* manual for instructions on setting up Expansion Unit addresses. **NOTE:** If the addresses for all units are not set up properly, the units will not operate properly.
Manual Button	Enable/disable the unit's Manual button located on the front panel of the unit.
Password	Set the unit's password. The password is case-sensitive and can be up to 9 printable characters.
Restore Factory Defaults	Resets the original settings for the MasterSwitch Plus unit. All unit and outlet properties are set to their defaults.
View Manufacturing Data	Displays the following information: Model Number, Manufacture Date, Hardware Rev, Firmware Rev, and Serial Number. These items cannot be configured.
View Self-Test Results	Allows you to display the results of the unit's last power-on self-test. The tests performed are: **Program Memory**: Confirms that the EPROM chip is working properly. **Non-Volatile Memory**: Confirms that the EEPROM chip is working properly.
Menu Timeout Period	Automatically logs you off after the specified period of inactivity.
Power On Time Delay	The time that the MasterSwitch Plus will delay after AC power is applied before starting the outlet's power-on sequence.

Outlet Properties Menu

Overview

MasterSwitch Plus has eight **Outlet Properties** menus—one for each outlet. To access these menus, enter an outlet number (1– 8) from the **Main menu**. The **Outlet Properties** menu varies according to the **Outlet Control** mode setting of the chosen outlet.

Graceful Shutdown menu items

Item	Definition
Outlet Name	Identifies each outlet.
Outlet Control Mode	Establishes mode for associated outlet.
Will Device Confirm	Indicates whether the device connected to the outlet can assert a shutdown signal.
Low Battery Warning Control	Selects the method MasterSwitch Plus uses for determining when to assert the outlet's Low Battery signal after the UPS has switched to battery operation.
UPS Low Battery Multiplier	A low battery signal is generated when the UPS's remaining battery runtime falls below this value multiplied by the UPS Low Battery Warning.
Restart Delay	The delay between removing power from an outlet due to a Graceful Shutdown and reapplying power to that outlet.
Power Off Delay	The time from the triggering event (such as a server confirming a shutdown) until power is removed from the outlet.
Power On Delay	Determines the time interval between the triggering event and power being applied to the outlet.
Reboot Duration	The delay between removing power from an outlet because of a reboot and reapplying power to an outlet.

Item	Definition
Battery Capacity Threshold	Sets the minimum percentage of Battery Capacity required of the UPS before an outlet can be turned on.
Enable/Disable UPS Alarms	Environment Alarm Masks: Indicates whether an outlet will react to a specific Environment alarm.
Select Another Outlet	Allows you choose another outlet to configure.
Alarm Action Delay	The amount of time that an Environment alarm must be asserted before the unit reacts to the alarm.

Annunciator menu items

Item	Definition
Outlet Name	Identifies each outlet.
Outlet Control Mode	Set the mode for the associated outlet: Graceful Shutdown or Annunciator.
Initial State	Defines the initial state of the outlet.
Alarm Action Delay	The amount of time that an Environment alarm must be asserted before the unit reacts to the alarm.
Enable/ Disable UPS Alarms	Environment Alarm Masks: Indicates whether an outlet will react to a specific Environment alarm. Settings are **Enabled** and **Disabled** for each of the 12 Environmental Monitoring Card alarms.
Select Another Outlet	Choose another outlet to configure.

Environmental Monitoring Card menu

Item	Description
Temp (Celsius)	Displays the current ambient temperature reading of each attached probe. Temperature is displayed in *nn.nn* degrees Celsius.
Humidity	Displays the current relative humidity reading of each attached probe. Humidity is displayed in *nnn.n*% relative humidity.
Low Limit	Allows you to disable or set the low alarm threshold for temperature and humidity for each probe. Temperature threshold is in degrees Celsius and humidity is in percentage of relative humidity. If alarm limits are exceeded, an alarm will be asserted to all outlets whose Enable/Disable Alarm settings for that alarm are set to Enabled.
High Limit	Allows you to disable or set the high alarm threshold for temperature and humidity for each probe. Temperature threshold is in degrees Celsius and humidity is in percentage of relative humidity. If alarm limits are exceeded, an alarm will be asserted to all outlets whose Enable/Disable Alarm settings for that alarm are set to Enabled.
Disable All Alarms	Allows you to control Environmental Monitoring Card operation. The options are: • **Yes** — All alarm limits are set to Disabled. MasterSwitch Plus will ignore all Environment alarms. • **No** — All alarm limits are reset to previous configuration.

Event-Related Menus

Introduction

Overview

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

- 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

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 NMS-specific IP address or domain name.
- 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 CTRL-L to access the 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 unit supports event-logging for all Network Management Card application firmware modules. To record and display Network Management Card and unit events, use any of the following to view the event log:

- Web interface
- Control console
- FTP
- SCP

Logged events

By default, any event which causes an SNMP trap will be logged, except for SNMP authentication failures. Additionally, the unit will log its abnormal internal system events. However, you can use the **Actions** option in the Web interface's **Events** menu to disable the logging of events based on their assigned severity level, as described in Event Actions (Web Interface Only).

Some System (Network Management Card) 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 System (Network Management Card) and MasterSwitch Plus (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 all the events that have been recorded since the log was last deleted, 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 or Device Manager, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

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

Note

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

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

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

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

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

1. At a command prompt, type `ftp` and the unit'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 for **User Name**, and **apc** is the default for **Password**.
3. Use the **get** command to transmit the text-version of the event log or data log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

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

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

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.
   - If you clear the data log, the event log records a deleted-log event.
   - 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.

Event Actions (Web Interface Only)

Overview

The **Actions** option is available only on the Web interface's **Events** menu. This option allows you to select which actions will occur for events that have a specified 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 a Syslog message notification.
- **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 to be sent. See Email action.

Click **Details** to access a complete list of the System (Network Management Card) and Device (MasterSwitch Plus) events that can occur, and then edit the actions that will occur for an individual event, as described in How to Configure Individual Events. Click **Hide Details** to return to the **Actions** option.

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

Severity levels

Except for some System (Network Management Card) events that do not have a severity level, events are assigned a default severity level based on their seriousness:

- **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 does not require immediate attention.
- **Severe:** Indicates an event that requires immediate attention. Unless resolved, severe Device and System events can cause incorrect operation of the unit or its Network Management Card.

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.

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

For more information about this log, see Event Log.

Syslog action

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

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.

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

Email action

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 the SNMP traps or e-mail enabled.

See Event Actions (Web Interface Only)

Trap receiver settings

To define which NMSs will receive traps:

- In the Web interface, use the **Recipients** option of the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu. Choose one of the trap receivers to modify, or select **Settings** and enable SNMP access for all trap receivers.

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/Domain Name** setting.
Receiver NMS IP/Domain Name	Identifies by IP address or Domain Name 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/Domain Name** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP/Domain Name** 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 System (DNS) servers, as described in DNS servers
- The DNS name of the SMTP server and the **From Address** setting for SMTP, as described in SMTP settings
- The e-mail addresses for a maximum of four recipients, as described in Email recipients

DNS servers

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

The unit will wait a maximum of 15 seconds for a response from the primary or (if specified) the secondary DNS server. If the unit 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 unit 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 unit. **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 unit (the recommended option, **Local**). This option ensures that the e-mail is sent before the 20-second time-out for the unit, and, if necessary, is retried several times. Also do one of the following:
	  • Enable forwarding at the SMTP server provided with the unit 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 unit 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 unit tries to send the e-mail only once.
	When the recipient uses the SMTP server provided with the unit, 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: MasterSwitch Plus: Outlet 01 on device turned on **Long**: Includes information about the unit and the event. For example: Name: TestLab Location: Building 3 Contact: DonAdams http://139.225.6.133 MasterSwitch Plus Ser #: WS0131005294 Date: 03/24/2005 Time: 16:09:48 Code: 0x0703 Warning - MasterSwitch Plus: Outlet 01 on device turned on

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 MasterSwitch Plus.

Note

Modifying events on the **Configure Event Action by Severity Level** page, will override any changes you have 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
0x0008	System: Warmstart	Severe
0x707	MasterSwitch: Device configuration changed on device Critical Rack	Informational

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

Data Menu (Web Interface Only)

Log Option

Use this option to access a log that stores information about the external Environmental Monitoring Unit, and the ambient temperature and relative humidity measured by the Environmental Monitor's sensors.

Use the **Data** menu's **Configuration** option to define how frequently data is sampled and stored in the data log. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.

See Configuration Option.

To retrieve the data log as a text file, see How to use FTP or SCP to retrieve log files.

Configuration Option

Use this option to access the “Data Log Configuration” page, which reports how much data can be stored in the data log. If you change the **Log Interval** setting, which defines how often data will be sampled and recorded in the data log, the report updates based on the new setting.

The minimum interval is **60** seconds; the maximum interval is **8** hours, **10** minutes, **15** seconds.

Network Menu

Introduction

Overview

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

- Define TCP/IP settings, including DHCP and BOOTP server settings, when a DHCP or BOOTP server is used to provide the needed TCP/IP values
- Use the Ping utility
- Define and display settings that affect the unit's settings for DNS, FTP, Telnet, SSH, SNMP, e-mail, Syslog, and the Web interface (SSL/TLS).

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
- FTP server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL

Option Settings

TCP/IP

Use this option to enable or disable BOOTP, and when BOOTP is disabled, to define the TCP/IP values that a unit needs to operate on the network:

- **System IP**: The IP address of the unit
- **Subnet Mask**: The subnet mask value
- **Default Gateway**: The IP address of the default gateway

For information about the watchdog role of the default gateway, see Resetting the network timer.

When BOOTP is enabled (the default setting), you can affect only the BOOTP setting. A BOOTP server will provide the MasterSwitch Plus with its TCP/IP settings whenever the unit is started, reset, or re-started.

Current TCP/IP settings fields. The current values for **System IP**, **Subnet Mask**, **Default Gateway**, the **MAC Address, Host Name,** and the **Domain Name** for the MasterSwitch Plus are displayed with the TCP/IP settings in the control console and Web interface. The **Ethernet Port Speed** is displayed on the Web interface only.

For more information on using BOOTP and DHCP, see Boot Mode.

Boot mode setting. This setting selects which method will be used to define the unit's TCP/IP settings whenever the unit turns on, resets, or restarts:

- **Manual**: Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) which are available only 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 unit 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.

For more information about how to use DHCP, see Boot Mode.

An **After IP Assignment** setting, by default, will 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 unit.

For information about the **After IP Assignment** setting, and other settings that affect how the unit 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 unit's **Host Name** and **Domain Name** values.
  - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the MasterSwitch Plus interface (except e-mail addresses) that accepts a domain name as input.
  - **Domain Name**: An Administrator needs to configure the domain name here only. In all other fields in the MasterSwitch Plus interface (except e-mail addresses) that accept domain names, the unit will add this domain name when only a host name is entered.

To override the expansion of a specified host name by the addition of the domain name, do one of the following:

- To override the behavior in all instances, set the domain name field in **Configure General Settings** to its default `somedomain.com` or to `0.0.0.0`.
- To override the behavior for a particular host name entry — for example when defining a trap receiver — include a trailing period. The MasterSwitch Plus recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully qualified domain name and therefore does not append the domain name.

- 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 unit in BOOTP or DHCP communication:
  - **Vendor Class**: Uses **APC**, by default.

– **Client ID**: Uses the unit's MAC address, by default.

If the Client ID is changed from the unit'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 unit's application firmware module type, by default. For example, a Symmetra module sets the **User Class** to **SY**, and a Smart-UPS/Matrix-UPS module sets it to **SUMX**.

• Two settings are available if **BOOTP only** is the Boot mode selection:

– **Retry Then Fail**: Defines how many times the unit will attempt to discover a BOOTP server before it stops (4, by default).

– **On Retry Failure**: Defines what TCP/IP settings will be used by the unit 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

Configure Domain Name Service Settings fields. Use these fields to define the IP addresses of the primary and secondary Domain Name System (DNS) used by the MasterSwitch Plus 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; view the result of the test DNS request in the **Last Query Response** field (which displays **No last query** or text describing the query result of the last test).

- Use the **Query Type** setting to select the method to use for the DNS query:
  - The URL name of the server (**Host**)
  - The IP address of the server (**IP**)
  - The fully qualified domain name (**FQDN**)
  - 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 **Host**, identify the URL
  - For **IP**, identify the IP address
  - For **FQDN**, identify the fully qualified domain name, formatted as *myserver*.*mydomain*.com.
  - For **MX**, identify the Mail Exchange address

- Enable or disable **Reverse DNS Lookup**, which is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic. With **Reverse DNS Lookup** enabled, when a network-related event occurs, reverse DNS lookup logs in the event log both the IP address and the domain name for the networked device associated with the event. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change much less frequently than IP addresses, enabling reverse DNS lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Ping utility (control console)

Select this option, available only in the control console, to check the network connection by testing whether a defined IP address or domain name responds to the Ping network utility.

By default, the IP address of the default gateway is used. However, you can use the IP address or domain name 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.

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. If you decide to use SCP for file transfer, be sure to disable the FTP server.

To configure SSH, see Telnet/SSH

Use the **Port** setting to identify the TCP/IP port that the FTP server uses to communicate with the unit. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5001** to **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. For example, for a port number of 5000 and a unit IP address of 152.214.12.114, you would use this command:

```
ftp 152.214.12.114:5000
```

To access a text version of the unit's event or data log, see How to use FTP or SCP to retrieve log files.

To use FTP to download configuration files:

- See File Transfer (control console only) if the files are on an FTP server of your company or agency.
- See Firmware file transfer methods if you are downloading files from the APC Web site.

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 automatically enables SCP.

When SSH is enabled and its port and encryption ciphers are 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.)

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 unit.

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 unit.

If you do not specify a host key file, the MasterSwitch Plus generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the APC Security Wizard creates. **The 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 unit.

Note

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the unit. 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 unit. • **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 unit. 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 unit IP address of 152.214.12.114, your Telnet client would require one or the other of the following commands:
	
	`telnet 152.214.12.114:5000`
	
	`telnet 152.214.12.114 5000`

SSH Port	Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the unit. 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**: SSH is currently disabled and is not using a host key. A host key may or may not be loaded. **NOTE:** A host key must be installed to the **/sec** directory of the unit. • **Generating**: The unit 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 unit). • **Valid**: The host key is valid. (If you install an invalid host key, the unit discards it and generates a valid one. However, a host key that the unit 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 unit 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 unit. **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 unit creates one when it reboots. **The 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 (**Settings** 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 as trap receivers, see Trap receiver settings.

See also

To use SNMP to manage a UPS or an Environmental Monitor, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide*, provided on the APC MasterSwitch *Utility* CD and on the APC Web site (www.apc.com).

Setting	Definition
Community Name	This setting defines the password (maximum of 15 characters) that an NMS defined by the **NMS IP/Domain Name** setting uses to access the channel.
NMS IP/ Domain Name	Limits access to the NMS specified by a domain name or to the NMSs specified by the format used for the IP address: • A domain name allows only the NMS at that location to have access. • 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.

Setting	Definition	
Access Type	Selects how the NMS defined by the **NMS IP/Domain Name** setting can use the channel, when that NMS uses the correct **Community Name**.	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged on to the control console or Web interface.
	Disabled	The NMS cannot use GETs or SETs.
	Write+	The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface.

Email

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

For more information about these settings, see SMTP settings; for more information about the e-mail capability of the MasterSwitch Plus, see E-mail Feature.

Syslog

By default, the unit can send messages to up to four Syslog servers whenever unit, Environmental Monitor, or UPS events occur. The Syslog servers, which must be specifically identified by their IP addresses or domain names, record the events that occur at network devices in a log that provides a centralized record of events.

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at **www.ietf.org/rfc/rfc3164.txt?number=3164**.

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.

Setting	Definition
General Settings	
Syslog	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code assigned to the unit's Syslog messages (**User**, by default). **NOTE:** Although several daemon-specific and process-specific selections are available, along with eight generic selections, **User** is the selection that best defines the Syslog messages sent by a unit.
Syslog Server Settings	
Server IP/ Domain Name	Uses specific IP addresses or domain names to identify which of up to four servers will receive Syslog messages sent by the unit. **NOTE:** To use the Syslog feature, at least **Server IP/Domain Name** must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the unit will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.

Setting	Definition
Local Priority (Severity Mapping)	
Map to Syslog's Priorities	Maps each of the severity levels (**Local Priority** settings) that can be assigned to UPS, environmental monitor, and unit 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 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 that 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 you want to assign to the test message.
2. Define the test message, using any text that is formatted as described in Syslog message format below. For example:
   `APC: Test message`
   meets the required message format.
3. Click **Apply** to have the unit 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) identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the unit.
- The Header includes a time stamp and the IP address of the unit.
- The message (MSG) part has two fields:
  - The Tag field, which is followed by a colon and a space, identifies the event type (APC, System, or UPS, for example)
  - The 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 MasterSwitch Plus:
  - 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 Sockets Layer (HTTPS): Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission, and provides authentication of the MasterSwitch Plus by means of 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 unit. 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 unit.
  - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload it to the location **\sec** on the unit

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 unit creates one when it reboots. **The 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 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 communication by HTTP with the unit. 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 unit IP address of 152.214.12.114, you would use this command: `http://152.214.12.114:5000`
HTTPS Port	Identifies the TCP/IP port used for communications by HTTPS with the unit. 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 unit IP address of 152.214.12.114, you would use this command: `https://152.214.12.114:6502`

Option	Description
SSL 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 unit. **NOTE:** If you install a certificate by using FTP or SCP, you must specify the correct location (**/sec**) on the unit. • **Generating**: The unit is generating a certificate because no valid certificate was installed. • **Loading**: A certificate is being loaded (activated on the unit). • **Valid**: A valid certificate was installed to or generated by the unit. (If you install an invalid certificate, the unit discards it and generates a valid one. However, a certificate that the unit generates has some limitations.)
Filename	You can create a server certificate with the APC Security Wizard and then upload it to the unit 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 unit. However, you must specify the correct location (**/sec**) on the unit. **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 unit creates one when it reboots. **The 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 unit, except if the server certificate was generated by default by the unit. For a default server certificate, the **Common Name (CN)** field displays the unit'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 unit; 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 unit, 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 unit. For a default server certificate, the **Common Name (CN)** field displays the unit'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 unit, 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 them 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 access parameters for the Administrator, Device Manager, and Read Only User accounts.
- Centrally administer remote access for each unit by using RADIUS (Remote Authentication Dial-in User Service)
- Synchronize the unit's real-time clock with a Network Time Protocol (NTP) server.
- Reset or restart the unit.
- Define the URL links available in the Web interface.
- Access hardware and firmware information about the unit.
- Set the units (Fahrenheit or Celsius) used for temperature displays.

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
- Outlet Usr Mgt
- RADIUS
- Identification
- Date & Time
- Tools
- Preferences (Web interface)
- Links (Web interface)
- About System

The **About System** options 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
Auto Logout	The number of minutes (3, by default) before a user is automatically logged off because of inactivity.
Separate values for Administrator, Device Manager, and Read Only User	
User Name	The case-sensitive name (maximum of 10 characters) used to log on at the control console or Web interface (**apc**, by default, for **Administrator**, **device**, by default, for **Device Manager User**, and **readonly**, by default, for **Read Only User**).
Password	The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but used to log into the Web interface only when **Basic** is selected for the **Authentication** setting (**apc** is the default password for the three account types).

Outlet Usr Mgt

Use the **Outlet Usr Mgt** option to set up user accounts that have access only to certain outlets

Web interface. Choose a user name, or choose **Add New User** to edit accounts.

Setting	Definition
User Name	The name of this user account **NOTE:** A user name in orange indicates that the user account has been disabled.
Password	Case-sensitive password for this user account
User Description	Identification or description of the outlet user
Account Status	Enables, disables, or deletes this user
Outlet Access	Selects the outlets to which users have access
Delete User	Deletes this user account

Control console. Select **System** from the control console menu. Then select **Manage Outlet Users** from the **User Manager** menu.

Setting	Definition
Add Outlet User Account Edit Outlet User Account	**User Name:** The name of this user account **Password:** Case-sensitive password for this user account **Description:** Identification or description of the outlet user
Delete Outlet User Account	Enter the name of the outlet user account you want to delete.
Disable Outlet User Account	Enter the name of the outlet user account to disable.

Setting	Definition
Enable Outlet User Account	Enter the name of the outlet user account to enable.
Edit Users Outlet Access	Select the outlets to which users have access: 1. Enter the outlet user name you want to modify. 2. Select the numbers of the outlets to which the outlet user will have access: -- Add outlet access by entering each number and pressing ENTER after each one. Enter a blank when finished. -- Remove outlet access by entering each number preceded by a minus sign (–) and pressing ENTER after each one. Enter a space when finished.
List Outlet Users Accounts	Displays outlet user name, status, description, and outlet access for each outlet user account.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting service. APC supports the authentication and authorization functions of RADIUS. Use this option to centrally administer remote access for each unit.

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

RADIUS user names are limited to 32 characters.

For more information on user permission levels, see Types of user accounts.

The RADIUS server and the MasterSwitch Plus must be configured before RADIUS authentication and authorization will operate properly.

RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

Configuring the MasterSwitch Plus.

RADIUS Setting	Definition
Access	**Local Only**: RADIUS is disabled. Local authentication is enabled.
	RADIUS then Local: RADIUS is enabled, and local authentication is enabled. Authentication is requested from the RADIUS server first; local authentication is used only if RADIUS authentication fails.
	RADIUS Only: RADIUS is enabled. Local authentication is disabled. **NOTE:** If RADIUS only is selected, the only way to recover if the RADIUS server is unavailable is by using a serial connection to the control console and changing the **Access** setting to **Local Only** or **RADIUS then Local**..
Primary Server	The server name or IP address of the main RADIUS server.
Primary Server Secret	The shared secret between the primary RADIUS server and the unit.
Secondary Server	The server name or IP address of the secondary RADIUS server.
Secondary Server Secret	The shared secret between the secondary RADIUS server and the unit.
Timeout	The time in seconds that the unit waits for a response from the RADIUS server.

Configuring the RADIUS server. You must configure your RADIUS server to work with the unit. The following example shows how to configure a RADIUS server for use with a Rack PDU. APC supports authentication and authorization of users by various RADIUS servers and does not recommend a specific RADIUS server.

1. Add the IP address of the Rack PDU to the RADIUS server client list (file).
2. The users must be configured with a Service-Type attribute. If no Service-Type attribute is configured, the user will have read-only access (on the Web interface only). There are two acceptable values for Service-Type: Administrative-User (6), which gives the user Administrator permissions, or Login-User (1), which gives the user Device permissions.

   The following examples may differ somewhat from the required content or format of your specific RADIUS server.

See your RADIUS server documentation for information about the RADIUS users file.

Example: (RADIUS users file)

```
#
UPSAdmin    Auth-Type = Local, Password = "admin"
     Service-Type = Administrative-User

UPSDevice   Auth-Type = Local, Password = "device"
     Service-Type = Login-User

UPSReadOnly Auth-Type = Local, Password = "readonly"
```

3. Vendor specific attributes (VSA) can also be used. This requires some dictionary entries. VSAs take precedence over standard RADIUS attributes.

Example: (RADIUS, dictionary.apc)

```
        #
        # dictionary.apc
        #
        #
        VENDOR    APC      318
#
# Attributes
#
ATTRIBUTE APC-Service-Type 1 integer APC
ATTRIBUTE APC-Outlets      2 string  APC

        VALUE APC-Service-Type Admin    1
        VALUE APC-Service-Type Device   2
        VALUE APC-Service-Type ReadOnly 3
        VALUE APC-Service-Type Outlet   4
```

Example: (RADIUS users file with VSAs)

```
VSAAdmin    Auth-Type = Local, Password = "admin"
APC-Service-Type = Admin

VSADevice   Auth-Type = Local, Password = "device"
APC-Service-Type = Device

VSAReadOnly Auth-Type = Local, Password = "readonly"
APC-Service-Type = ReadOnly

# Give user access to MasterSwitch outlets 1, 2 and 3.
VSAOutlet   Auth-Type = Local, Password = "outlet"
APC-Service-Type = Outlet,
    APC-Outlets = "1,2,3"
```

For more information on user permission levels, see Types of user accounts.

Identification

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

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* provided on the APC MasterSwitch *Utility* CD.

Date & Time

Use this option to set the date and time used by the MasterSwitch Plus. 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 MasterSwitch Plus.

An **Apply Local Computer Time to Switched Rack PDU** 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 MasterSwitch Plus.

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 or domain name of the primary NTP server.
Secondary NTP Server	Identifies the IP address or domain name 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 unit is located.
Update Interval	Defines how often, in weeks, the unit 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

Initiating an action. Use this drop-down list in the Web interface or the equivalent menu options in the control console to restart the interface of the unit, to reset some or all of its configuration settings to their default values, or to delete SSH Host Keys and SSL Certificates.

Action	Definition
Reboot Management Interface	Restarts the interface of the unit.
Reset to Defaults	Resets all configuration settings. **NOTE:** For information about how this affects the **Boot mode** setting, see this table's description of **Reset Only TCP/IP to Defaults**.
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 unit'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 unit so that you can reconfigure these components of your security system.

Uploading an initialization file (Web interface only). To transfer configuration settings from a configured unit to the current unit, export the .ini file from the configured unit, select the **Tools** menu on the current unit, browse to the file, and click **Upload**. The current unit imports the file and uses it to set its own configuration. The **Status** field reports the progress of the upload.

File Transfer (control console only). The **File Transfer** option of the **Tools** menu provides two methods for file transfer over the network and one for file transfer through a serial connection to the unit.

Option	Description
XMODEM	Allows you to transfer either an .ini file or a firmware upgrade file to a unit using a terminal-emulation program. This option is available only when you use a local connection to the control console. See Local access to the control console.
FTP Client	Use one of these two options to transfer either an .ini file or a firmware upgrade file from an FTP or TFTP server of your organization (company, agency, or department) to the current unit. These options assume that your organization has a centralized system for configuring or upgrading APC units. For **FTP Client**, you are prompted for a user name and password. For either option, you are then prompted for the server address and the file to transfer. After you supply that required information, the unit transfers the file.
TFTP Client	

Preferences (Web interface)

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

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 Web Site) • **http://testdrive.apc.com** (Testdrive Demo) • **http://rms.apc.com** (Remote Monitoring)
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**).

About System

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

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

This information is set at the factory and cannot be changed.

The control console also includes fields for system **Flash Type**, and **Type**, **Sector**, and **CRC16** for each module.

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

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the MasterSwitch Plus 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 • Domain Name • NMS IP filters • Agent Enable/Disable • 4 access communities with read/write/disable capability	The domain name restricts access only to the NMS as that location, and the NMS IP filters allow access only from designated IP addresses. • 162.245.12.1 allows only the NMS with that IP address to have access. • 162.245.12.255 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 transferred without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Sockets 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 • Secure Sockets 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). SSL and TLS are available on Web browsers supported for the MasterSwitch Plus and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

RADIUS.

Security Access	Description
Available methods: • Centralized authentication of access rights • A server secret shared between the RADIUS server and the unit	RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting service used to centrally administer remote access for each unit.

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the unit, 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 MasterSwitch Plus. 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 MasterSwitch Plus that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

To ensure that data and communication between the MasterSwitch Plus 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 Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- 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 Sockets Layer (SSL)/Transport Layer Security (TLS).

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 MasterSwitch Plus) 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 MasterSwitch Plus) 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.

To create a host key, see Create an SSH Host Key.

- The MasterSwitch Plus 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 unit, 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 Sockets Layer (SSL)/Transport Layer Security (TLS)

For secure Web communication, you enable Secure Sockets 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 MasterSwitch Plus. Hypertext Transfer Protocol over Secure Sockets 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 MasterSwitch Plus 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 MasterSwitch Plus). 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 Web site (www.apc.com), 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 unit.

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

To create certificates and certificate requests, see Create a Root Certificate & Server Certificates and Create a Server Certificate and Signing Request.

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.

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. 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 MasterSwitch Plus supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the MasterSwitch Plus (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 the auto-generated 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.

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

Method 1: Use the auto-generated default certificate. When you enable SSL, you must reboot the unit. During rebooting, if no server certificate exists on the unit, the unit generates a default server certificate that is self-signed but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**
  - Before they are transmitted, the user name and password for unit access and all data to and from the unit 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 unit 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 unit, 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 unit has the unit's serial number in place of a valid *common name* (the DNS name or the IP address of the unit). Therefore, although the unit 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 unit 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 unit.
- A *server certificate* that you upload to the unit. 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 unit sending or requesting data:

- To identify the unit, the browser uses the *common name* (IP address or DNS name of the unit) 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 unit access and all data to and from the unit 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 unit enables SSL to authenticate that data are being received from and sent to the

correct unit. 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 unit'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 unit.

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 unit access and all data to and from the unit 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 unit.
  - 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 unit enables SSL to authenticate that data are being received from and sent to the correct unit. 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 unit 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.

Using the APC Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an APC MasterSwitch Plus). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the MasterSwitch Plus supports more secure methods of authentication.

- Secure Sockets Layer (SSL), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the unit.
- Secure SHell (SSH), used for remote terminal access to the unit's control console, uses a public *host key* for authentication rather than a digital certificate.

How certificates are used. Most Web browsers, including all browsers supported by the MasterSwitch Plus, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the unit) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser. For this authentication to occur:

- Each MasterSwitch Plus with SSL enabled must have a server certificate on the unit itself.
- Any browser that is used to access the unit's Web interface must contain the CA root certificate that signed the server certificate.

If authentication fails, the browser prompts you on whether to continue despite the fact that it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the unit generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the unit.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the MasterSwitch Plus) each time an SSH client contacts the unit. Each MasterSwitch Plus with SSH enabled must have an SSH host key on the unit itself.

Files you create for SSL and SSH security

Use the APC Security Wizard to create the following components of an SSL and SSH security system:

- The server certificate for the MasterSwitch Plus, if you want the benefits of authentication that such a certificate provides.You can create either of the following types of server certificate:
  - A server certificate signed by a custom CA root certificate also created with the APC Security Wizard. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
  - A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate.
- An SSH host key that your SSH client program uses to authenticate the unit when you log on to the control console interface.

All public keys for SSL certificates and all host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys. If you do not create and use SSL server certificates and SSH host keys with the APC Security Wizard, the unit generates 768-bit RSA keys.

Only APC server management and key management products can use server certificates, host keys, and CA root certificates created by the APC Security Wizard. These files will not work with products such as OpenSSL® and Microsoft IIS.

Create a Root Certificate & Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.

Note

The public RSA key that is part of a certificate generated by the APC Security Wizard is 1024 bits. (The default key generated by the unit, if you do not use the Wizard, is 768 bits.)

- Create a CA root certificate that will be used to sign all server certificates to be used with MasterSwitch Plus units. During this task, two files are created.
  - The file with the **.p15** extension is an encrypted file which contains the Certificate Authority's private key and public root certificate. This file signs the server certificates.
  - The file with the **.crt** extension, which contains only the Certificate Authority's public root certificate. You load this file into each Web browser that will be used to access the MasterSwitch Plus so that the browser can validate the server certificate of the unit.
- Create a server certificate, which is stored in a file with a **.p15** extension. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the MasterSwitch Plus.
- For each MasterSwitch Plus that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the CA root certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC MasterSwitch *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled "Step 1," select **CA Root Certificate** as the type of file to create.
4. Enter a name for the file that will contain the Certificate Authority's public root certificate and private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled "Step 2," provide the information to configure the CA root certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter an identifying name of your company or agency; use only alphanumeric characters, with no spaces.

   By default, a CA root certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note

The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate has been created and instructs you on the next tasks.
   – This screen displays the location and name of the **.p15** file that you will use to sign the server certificates.
   – This screen also displays the location and name of the **.crt** file, which is the CA root certificate that you will load into the browser of each user who needs to access the unit.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the unit.

See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. On the **Content** tab in the **Internet Options** dialog box, click **Certificates** and then **Import**.
3. The Certificate Import Wizard will guide you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure Create a Root Certificate & Server Certificates.

Create an SSL Server User Certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **SSL Server Certificate** as the type of file to create.
3. Enter a name for the file that will contain the server certificate and the private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
4. Click the **Browse** button, and select the CA root certificate created in the procedure Create a Root Certificate & Server Certificates. The CA Root Certificate is used to sign the Server User Certificate being generated.
5. On the screen labeled Step 2, provide the information to configure the server certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP address or DNS name of the server (MasterSwitch Plus). Because the configuration information is part of the signature, it cannot be exactly the same as the information you provided when creating the CA root certificate; the information you provide in some of the fields must be different.

   Note

   By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note

The information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration; some other configuration information must also differ.)

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the MasterSwitch Plus. It displays the location and name of the Server Certificate, which has a **.p15** file extension and contains the unit private key and public root certificate.

Load the server certificate to the unit. Perform these steps:

1. On the **Network** menu of the Web interface of the MasterSwitch Plus, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate & Server Certificates. (The default is **C:\Program Files\American Power Conversion\APC Security Wizard**.)

Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the unit. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the unit. For SCP, the command to transfer a certificate named **cert.p15** to a unit with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR).The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
  - The file with the **.p15** extension contains the MasterSwitch Plus unit's private key.
  - The file with the **.csr** extension contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** extension.
- Load the server certificate onto the MasterSwitch Plus.
- For each MasterSwitch Plus that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR). Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC MasterSwitch *Utility* CD.

2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled "Step 1," select **Certificate Request** as the type of file to create.
4. Enter a name for the file that will contain the MasterSwitch Plus unit's private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the certificate signing request (CSR) with the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the MasterSwitch Plus.

By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate signing request has been created and displays the location and name of the file, which has a **.csr** extension.

8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.

See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the signed certificate. When the external Certificate Authority returns the signed certificate, perform these steps to import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the MasterSwitch Plus. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **Import Signed Certificate**.
3. Browse to and select the signed server certificate that you received from the external Certificate Authority. The file has a **.cer** or **.crt** extension.
4. Browse to and select the file you created in step 4 of the task, Create the Certificate Signing Request (CSR). This file has a **.p15** extension, contains the MasterSwitch Plus unit's private key, and, by default, is located in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the unit. The file must have a **.p15** extension.
6. Click **Next** to generate the server certificate. The certificate's **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the MasterSwitch Plus. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the unit's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the unit. Perform these steps:

1. On the **Network** menu of the Web interface of the MasterSwitch Plus, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure Import the signed certificate. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the unit. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the unit. For SCP, the command to transfer a certificate named **cert.p15** to a unit with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the MasterSwitch Plus generates a 768-bit RSA key when it reboots. Host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys.

- Use the APC Security Wizard to create a host key, which is encrypted and stored in a file with **.p15** extension.
- Load the host key onto the unit.

The procedure

Create the host key. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC MasterSwitch *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **SSH Server Host Key** as the type of file to create.
4. Enter a name for the file that will contain the host key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Click **Next** to generate the Host Key
6. The summary screen displays the SSH version 1 and version 2 fingerprints, which are unique for each host key and identify the host key. After you load the host key onto the unit, you can verify that the

correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the unit, as displayed by your SSH client program.

7. The last screen verifies that the host key has been created and instructs you on the next task, to load the host key to the MasterSwitch Plus. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the unit. Perform these steps:

1. On the **Network** menu of the Web interface of the MasterSwitch Plus, select the **Telnet/SSH** option.
2. In the **SSH User Host Key File** section of the page, browse to the host key, the **.p15** file you created in the procedure Create the host key. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)
3. On the **SSH Host Key Fingerprint** section of the page, note the fingerprint for the version (or versions) of SSH you are using. Then log on to the unit through your SSH client program, and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the unit. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the unit. For SCP, the command to transfer a host key named **hostkey.p15** to a unit with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\hostkey.p15
```

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Devices that contain embedded Network Management Cards

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card through a direct connection from the serial port of your computer to the device that contains the card.

The Wizard can discover and configure Network Management Cards only if they are on the same network segment as the computer that is running the Wizard.

System requirements

The Wizard runs on Windows NT®, Windows 2000, Windows 2003, and Windows XP workstations.

Install the Wizard

Automated installation

If autorun is enabled on your CD-ROM drive, the installation program starts automatically when you insert the CD.

Manual installation

If autorun is not enabled on your CD-ROM drive, run **setup.exe** in the Wizard directory on the CD, and follow the on-screen instructions.

You can also download the latest version of the APC Device IP Configuration Wizard from the APC web site, **www.apc.com** and run **setup.exe** from the folder to which you downloaded it.

Use the Wizard

Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

1. Contact your network administrator to obtain valid TCP/IP settings to use.
2. If you are configuring multiple unconfigured Network Management Cards, obtain the MAC address of each one so that you can identify each Network Management Card that the Wizard discovers. (The Wizard displays the MAC address for a discovered card on the same screen on which you then enter the TCP/IP settings.)
   - For Network Management Cards that you install, the MAC address is on a label on the bottom of the card.
   - For embedded Network Management Cards, the MAC address is on a label on the device containing the card — for example, usually on the side of a device that you mount in a rack.

   You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or with the device containing an embedded Network Management Card.

Run the Wizard to perform the configuration. To discover and configure, over the network, installed or embedded Network Management Cards that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Network Management Card that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card identified by the MAC address at the top of the screen. Then click **Next >**.
4. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
5. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
6. The Wizard searches for another installed or embedded but unconfigured Network Management Card. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card.
   - To skip configuring the card whose MAC address is currently displayed, click **Cancel**.
   - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 4.

Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable that came with the Network Management Card or with the device that contains an embedded Network Management Card.
   a. Connect one end to an available communications port on your computer. Make sure no other application is using the port.
   b. Connect the other end to the serial port of the card or device.
3. From the **Start** menu, launch the Wizard application.
   – If the Network Management Card is not configured, wait for the Wizard to detect it.
   – If you are assigning basic TCP/IP settings serially to a Network Management Card, click **Next>** to move to the next screen.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the Network Management Card. Then click **Next >**.
6. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
7. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
8. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the card or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of a MasterSwitch Plus unit's current configuration and export that file to another MasterSwitch Plus or to multiple MasterSwitch Plus units.

1. You configure a MasterSwitch Plus to have the settings you want to export.
2. You retrieve the .ini file from that unit.
3. You then customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. You use any of the file transfer protocols supported by the MasterSwitch Plus to transfer the copied file to one or more additional units. (To transfer the file to multiple units simultaneously, write an FTP script that repeats the steps for transferring the file to a single unit.)
5. Each receiving MasterSwitch Plus stores the file temporarily in its flash memory, uses it to reconfigure its own unit settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from an MasterSwitch Plus contains the following:

- *section headings*, which are category names enclosed in brackets ([ ]), and under each section heading, *keywords,* which are labels describing specific unit settings.

Only section headings and keywords supported for the specific device (in this case, the unit) from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
- The `Override` keyword, with its default value, prevents one or more keywords and their device-specific values from being exported. In the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the unit) blocks the exporting of the values for the keywords `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.
- You must edit the section `[SystemDate/Time]` if you want to set the system date and time of a receiving unit or cause that unit to use an NTP Server to set its date and time.

See Customizing for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one MasterSwitch Plus and export them to one or more MasterSwitch Plus units.

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

1. Configure an unit with the settings you want to export.

   To avoid errors, configure the unit by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the unit you configured.
   a. Open a connection to the unit, using its IP Address. For example:

      ```
      ftp> open 158.165.2.132
      ```

   b. Log on, using the Administrator user name and password configured for the unit.
   c. Retrieve the config.ini file containing the unit's current settings:

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

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

To create batch files and use an APC utility to retrieve configuration settings from multiple units and export them to other units, see *Release Notes: ini File Utility, version 1.0*, provided on the APC MasterSwitch *Utility* CD and on the APC Web site (www.apc.com).

Customizing. You must customize the file to change at least the TCP/IP settings before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
   - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
     - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
     - For greater accuracy, if the MasterSwitch Plus units receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows:

       ```
       NTPEnable=enabled
       ```
   - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The copy, which you will export to other units, can have any file name up to 64 characters and must have the .ini suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Exporting the file to a single unit. To export the .ini file to another MasterSwitch Plus, use any of the file transfer protocols supported by MasterSwitch Plus units (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

1. From the folder containing the customized .ini file and its copy, use FTP to log in to the unit to which you are exporting the .ini file. For example:

   ```
   ftp> open 158.165.4.135
   ```

2. Export the copy of the customized .ini file. The receiving unit accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

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

Exporting the file to multiple units. To export the .ini file to multiple MasterSwitch Plus units:

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

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the APC MasterSwitch *Utility* CD.

The Upload Event and its Error Messages

The event and its error messages

The following system event occurs when the receiving MasterSwitch Plus completes using the .ini file to update its settings.

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

This event has no default severity level.

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.

The export to and the subsequent upload by the receiving unit succeeds even if there are errors.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the unit stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A feature might not be supported for the device from which you retrieve the configuration settings or might not be supported for the device to which you export the configuration settings. In this case, the user configuration file contains, under the section name for that feature, a message stating that the feature is not supported. No keywords and values are listed, and that feature will not be configured on any device to which you export the user configuration file.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See Contents of the .ini file for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other units. Therefore, you can ignore these error messages. To prevent these error messages from occurring, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Using the Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for exporting .ini files, you can choose to update unit settings by using the Device IP Configuration Wizard.

For a detailed description of how to update the configuration settings of one or more MasterSwitch Plus units using the Device IP Configuration Wizard, see APC Device IP Configuration Wizard.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the MasterSwitch Plus 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 used to provide the network settings for the unit depends on **Boot mode**, a **TCP/IP** option in the **Network** menu. To use a DHCP server to provide the network assignment for the unit, **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.

For more details on DHCP and DHCP options, see RFC2131 and RFC2132 at **http://www.ietf.org/rfc**.

DHCP & BOOTP boot process

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

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

   Note

   To configure the MasterSwitch Plus 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 MasterSwitch Plus settings.

3. If the MasterSwitch Plus 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 MasterSwitch Plus 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

MasterSwitch Plus settings

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

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 the selection that reflects the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**).
- **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 MasterSwitch Plus will repeat the DHCP request if it does not receive a valid response. By default, the number of retries is 0, which sets the MasterSwitch Plus to continue repeating the DHCP request indefinitely.

DHCP response options

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

The unit 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 unit 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 unit can accept the lease.

Use the **DHCP Cookie Is** setting described in MasterSwitch Plus 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 MasterSwitch Plus 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 MasterSwitch Plus accepts the DHCP response. Whenever the unit restarts, it will request its network assignment (TCP/IP settings) from a DHCP server only.

For more information about the **After IP Assignment**, see MasterSwitch Plus 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 MasterSwitch Plus 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 unit.
- **Subnet Mask** (option 1): Provides the subnet mask value needed by the unit to operate on the network.
- **Default Gateway** (option 3): Provides the default gateway address needed by the unit 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 unit 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 unit must wait after an IP address lease is assigned before it can seek to rebind that lease.

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

File Transfers

Introduction

Overview

The MasterSwitch Plus automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

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

This chapter describes how to transfer firmware files to MasterSwitch Plus units.

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

To verify a file transfer, see Verifying Upgrades and Updates.

Upgrading Firmware

Benefits of upgrading firmware

Upgrading the firmware on the MasterSwitch Plus has the following benefits:

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

Firmware files (MasterSwitch Plus)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

The APC Operating System (AOS) and application module files used with the MasterSwitch Plus share the same basic format:

`apc_hw0x_type_version.bin`

- `apc`: Indicates that this is an APC file.
- `hw0x`: Identifies the version of the MasterSwitch Plus that will run this binary file.
- *`type`*: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the MasterSwitch Plus.
- *`version`*: The version number of the application file. For example, a code of 264 would indicate version 2.6.4.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system

- The version of the tool on the APC MasterSwitch *Utility* CD will upgrade your device to the latest AOS and application modules available when the CD was released.
- If a later firmware upgrade is available, you can obtain an updated version of the tool at no cost from the support section of the APC web site **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product (in this case, your unit) and download the automated tool, not the individual firmware modules.

If the AOS firmware module you already have is a 1.*x.x* version, the executable tool must perform two consecutive upgrades:

- The first upgrade is from version 1.*x.x* to the latest available 2.0.*x* version of the AOS firmware module.
- The second upgrade is from the 2.0.*x* version to the most recently released version of the AOS module.

The tool therefore contains firmware modules for both upgrades.

Each upgrade tool is specific to an APC product type. Do not use the tool from one product CD to upgrade firmware of a different APC product. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of your units manually, i.e., by using the separate APC firmware modules (AOS module and application module).

If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in Automated upgrade tool for Microsoft Windows systems to upgrade the firmware of a MasterSwitch Plus automatically over the network. This tool automates the entire upgrade process, even if your current firmware is a 1.*x.x* version.

When performing a manual upgrade, not using the automated tool, you cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.*x.x* to firmware version 2.1.0 or later. The upgrade attempt will fail. You must first upgrade to the latest availaible 2.0.*x* version of the AOS module and then to the later version.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC Web site **www.apcc.com/tools/download**.

Firmware file transfer methods

To upgrade the firmware of a MasterSwitch Plus:

- From a networked computer running a Microsoft Windows operating system, you can use the automated firmware upgrade tool on your CD or downloaded from the APC Web site.
- From a networked computer on any supported operating system, you can use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a MasterSwitch Plus that is not on your network, you can use XMODEM through a serial connection to transfer the individual AOS and application firmware modules from your computer to the MasterSwitch Plus.

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for a unit, you must transfer the APC Operating System (AOS) module to the unit before you transfer the application module.

For more information about the firmware modules, see Firmware files (MasterSwitch Plus).

Use FTP or SCP to upgrade one unit

Instructions for using FTP. For you to be able to use FTP to upgrade a single MasterSwitch Plus over the network:

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

To use FTP to upgrade the unit:

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 MasterSwitch Plus, for example, might be the following:

   –`apc_hw02_aos_264.bin`

   –`apc_hw02_app_262.bin`

2. Open an FTP client session:

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

3. Type `open` and the MasterSwitch Plus's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default of **21**, you must use the non-default value in the FTP command.

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

   b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the unit'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 unit 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_264.bin
```

6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 5, but in step 5, use the application module file name instead of the AOS module.

Instructions for using SCP. To use Secure CoPy (SCP) to upgrade the firmware for one unit:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the unit. The following example assumes a unit IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_264.bin**.)

```
scp apc_hw02_aos_264.bin apc@158.205.6.185:apc_hw02_aos_264.bin
```

3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the unit.

How to upgrade multiple units

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple units and export them to other units.

See *Release Notes: ini File Utility, version 1.0*, provided on the APC MasterSwitch *Utility* CD and on the APC Web site (www.apc.com).

Use FTP or SCP to upgrade multiple units. To upgrade multiple MasterSwitch Plus units using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in Use FTP or SCP to upgrade one unit.

Use XMODEM to upgrade one unit

You cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.*x.x* to 2.1.0 or later. The upgrade attempt will fail.

To upgrade the AOS firmware module of an APC device from version 1.*x.x* to 2.1.0 or later, first upgrade the module to the latest available version 2.0.*x* AOS firmware module. Then upgrade it again, this time from version 2.0.*x* to the 2.*x.x* version you want.

If your APC device is running a 2.0.*x* of the AOS firmware module already, you can upgrade directly to version 2.1.0 or a later version.

To use XMODEM to upgrade the firmware for a single MasterSwitch Plus that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from the support section of the APC web site **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service which uses that port.
3. Connect the smart-signaling cable that came with the unit to the selected port and to the serial port at the unit.
4. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
5. Press ENTER to display the **User Name** prompt.
6. Enter your Administrator user name and password. The default for

both is **apc**.

7. Start an XMODEM transfer:
   a. Select option 3—**System**
   b. Select option 4—**File Transfer**
   c. Select option 2—**XMODEM**
   d. Type `Yes` at the prompt to continue with the transfer.
8. Select the appropriate baud rate. A higher baud rate causes faster firmware upgrades. Also, change the terminal program's baud rate to match the one you selected, and press ENTER.
9. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The unit will automatically restart.
10. Repeat **step 3** through **step 8** to install the application module. In **step 8**, substitute the application module file name for the AOS module file name.

For information about the format used for application modules, see Firmware files (MasterSwitch Plus).

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

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

You can also verify the versions of the upgraded APC Operating System (AOS) and application modules by using the **About System** option in the **System** menu of the control console or in the **Help** menu of the Web interface, or by using an SNMP GET to the MIB II **sysDescr** OID

Product Information

Warranty and Service

Limited warranty

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

Warranty limitations

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

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

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

Obtaining service

To obtain support for problems with your MasterSwitch Plus:

1. Note the serial number and date of purchase. To find the serial number of the MasterSwitch Plus, use the **About System** menu option, or look on the bottom of the unit.
2. Contact Customer Support at a phone number located at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

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

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

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

990-6012D **05/2005**