MasterSwitch

Power Distribution Unit

AP9211
AP9212
AP9217
AP9218

User's Guide

APC®

Contents

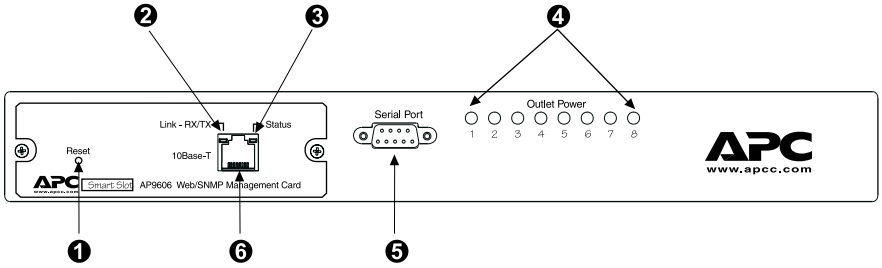
Contents

Contents

Introduction

Product Description

Front panel



❶	Reset Button	Re-initializes the MasterSwitch PDU without affecting the outlet state.
❷	Status LED	Indicates the status of the Ethernet LAN connection and the state of the management card, as described in **LEDs on page 2**.
❸	Link-RX/TX LED	
❹	Eight Outlet Power LEDs	Indicates whether the associated outlet is on.
❺	Serial Port	Connects the MasterSwitch PDU to a terminal emulator program to access the Control Console.
❻	RJ-45 Port	Connects the MasterSwitch PDU to an Ethernet LAN using the 10Base-T communication cable. This connection allows configuration of the MasterSwitch PDU through the Web, Telnet, or SNMP.

Continued on next page

Introduction

Product Description *continued*

LEDs

Each outlet has a corresponding LED that indicates the state of the outlet, and two LEDs indicate the status of the entire unit. The following table describes the conditions indicated by the LEDs.

LED	Status	Description
Outlet LED	On	The Outlet is on.
	Off	The Outlet is off.
Status	Off	The MasterSwitch PDU has no power.
	Green	The MasterSwitch PDU has valid network settings.
	Flashing Green	The MasterSwitch PDU does not have valid network settings.
	Red	A hardware failure has been detected in the MasterSwitch PDU.
	Blinking Red	The MasterSwitch PDU is making BOOTP requests.
Link-RX/TX	Off	The device that connects the MasterSwitch PDU to the network (a router, hub, or concentrator) is off or is not operating correctly.
	Flashing Green	The MasterSwitch PDU is receiving data packets from the network.

Continued on next page

Introduction

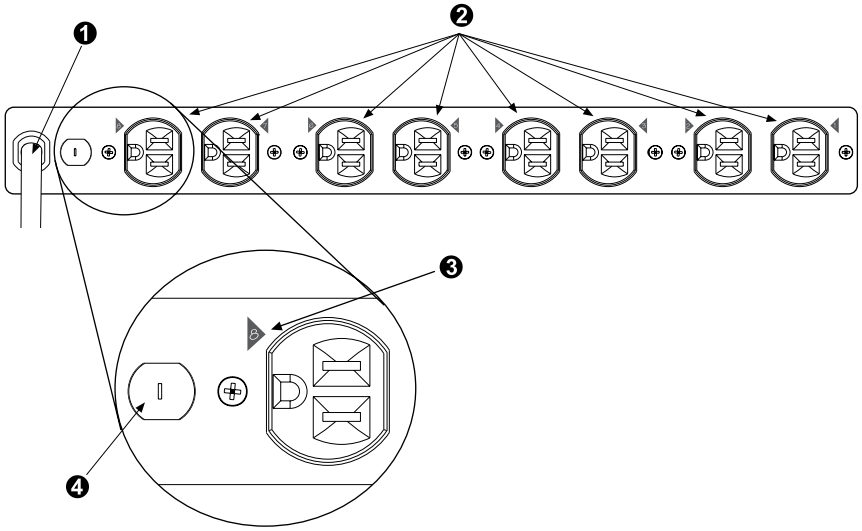
Product Description *continued*

Rear panel

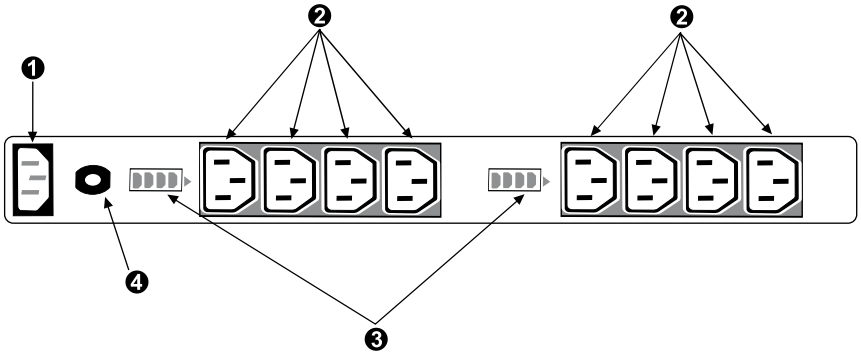
The following table lists the features of the MasterSwitch rear panel shown in the figures on this page.

❶	Power Cord/ IEC Inlet
❷	Outlets
❸	Outlet Label
❹	Circuit Breaker

The following figure shows the MasterSwitch (AP9211/AP9217) rear panel with NEMA 5-15 outlets.



The following figure shows the MasterSwitch (AP9212/ AP9218) rear panel with IEC-320 C13 outlets.



Introduction

Initial Setup

Required network settings

You must configure the following network settings of the MasterSwitch PDU before it can operate on a network:

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

Note: If a default gateway is not present, enter an IP address of a computer that is on the same subnet and that is always active.

Configuring TCP/IP settings

To configure TCP/IP settings, see **TCP/IP on page 15** and see the MasterSwitch *Installation and Quick Start Manual*, included in printed form with the MasterSwitch PDU and in Portable Document Format (***Install.pdf***) on this CD-ROM.

Customizing your configuration

After you configure MasterSwitch network settings, no further configuration is required. The remaining MasterSwitch properties are pre-configured to default settings at the factory. However, you may want to customize these properties for your application. For more information, see **Managing the MasterSwitch PDU on page 5**.

Auto-configuration

The management card within the MasterSwitch PDU supports an auto-configuration utility that you can use to create a configuration file, which you can then download to other MasterSwitch PDUs, either to individual units one at a time or to multiple units at the same time. For more information, see the ***Management Card Addendum*** (***addendum.pdf*** on the MasterSwitch CD-ROM).

Managing the MasterSwitch PDU

Management Interfaces

Management Options

After you configure a MasterSwitch PDU with the proper network settings, you can manage the unit remotely through its Web, Telnet Control Console, SNMP, and WAP interfaces.

You can also use the Control Console to manage a MasterSwitch PDU locally through a serial connection.

Only one user at a time can access a MasterSwitch PDU. Serial interface users (using a terminal emulator) have precedence over Telnet users, and Telnet users have precedence over Web and WAP users.

Web interface

To access and log on to the Web interface of the MasterSwitch PDU:

1. In the URL Location field of the Web browser, do one of the following:
   - If the Web port of the MasterSwitch PDU is set to the default value of 80, enter `http://` followed by the unit's IP address. The following example shows a typical IP address:

     `http://170.241.17.51`
   - If the Web port of the MasterSwitch PDU is set to a value other than the default of 80, enter the System IP address (the IP address of the unit) followed by a colon and the configured Web port value (8000 in the following example).

     `http://170.241.17.51:8000`
   - If there is a DNS server entry for the MasterSwitch PDU, you can choose to enter the DNS name to access the unit.

Continued on next page

Managing the MasterSwitch PDU

Management Interfaces *continued*

Web interface, continued

2. Respond to the user name and password prompts. The default for both the Administrator user name and the Administrator password is *apc* (lowercase). After you log on, you can change the user name, password, and time-out values through the System menu. See **User Manager on page 18**.

Note: Some Web interface features (data verification, Assistant Online, and MD5 authentication) require that you enable JavaScript or Java on your web browser, and MD5 authentication also requires that you have cookies enabled.

Control Console interface

In addition to or instead of using the Web interface, you can use the Control Console to manage the MasterSwitch PDU by one of the following modes of access:

- Telnet, for remote management.
- A serial interface, for local management.

Telnet. To access the unit's Control Console:

1. Choose **Connect**, then **Remote Server**.
2. Type the IP address of the MasterSwitch PDU.
3. Click the Connect button.

Continued on next page

Managing the MasterSwitch PDU

Management Interfaces *continued*

Control Console interface, continued

Serial Interface. To access the unit's Control Console, use the supplied null-modem cable to connect the serial port of the computer to the serial port on the MasterSwitch PDU, and set the terminal port to the following communication settings:

Baud Rate	2400
Data Bits	8
Stop Bits	1
Parity	None
Handshaking	None
Local Echo	Off
Terminal Type	ANSI (VT100)

Logging on. To log on to the Control Console using either Telnet or a serial interface, respond to the user name and password prompts.The default for both the Administrator user name and the Administrator password is *apc* (lowercase).

> **Note:** You can change the user name, password, and time-out values through the System menu. See **User Manager on page 18**.

Using menu items. All menus of the Control Console list items by number and name.

- To select an item, type the number, and press ENTER.
- For menus that configure value, always use the **Accept Changes** option to save any changes that you make.

SNMP interface

MasterSwitch fully supports SNMP—all unit and outlet properties are configurable through SNMP. For instructions on how to use SNMP to manage MasterSwitch, see the *Mibguide.pdf* and the *NMS.pdf* files in the **Snmp** folder on the CD.

Continued on next page

Managing the MasterSwitch PDU

Management Interfaces *continued*

WAP Interface

To access and log on to the WAP (Wireless Application Protocol) interface of the MasterSwitch PDU:

1. In the URL Location field of the Micro browser:
   Enter the unit's IP address followed by `wap.wml`. The following example shows a typical address:
   ```
   123.456.78.9/wap.wml
   ```
2. Respond to the user name and password prompts. If it has not been changed since purchase, the default for both the Administrator user name and the Administrator password is *apc* (lowercase).

Depending on the level of access (Administrator, Device Manager or Outlet User), the WAP interface will display outlets assigned to the user who logged on and will offer the following control options for the MasterSwitch unit:

- immediate on
- immediate off
- reboot
- master control of all outlets (All).

Note: The character preceding each outlet indicates whether the outlet is on (+) or off (–).

Managing the MasterSwitch PDU

Password-Protected Accounts

Account access

There are up to 16 Outlet User accounts, one Administrator account, and one Device Manager account. Each type of account provides a different level of access to the management menus.

- Each Outlet User account has access only to the outlets assigned to it.
- The Administrator and Device Manager accounts have access to all outlets.
- The Administrator account can configure and manage all other accounts.

Menu Items	Account Type		
	Administrator	Device Manager	Outlet User
Outlets	Yes	Yes	Yes
MasterSwitch	Yes	Yes	No
Event Log	Yes	Yes	No
Network	Yes	No	No
System	Yes	No	No
Logout	Yes	Yes	Yes
Help	Yes	Yes	Yes
Links	Yes	Yes	Yes

For instructions on configuring Device Manager and Outlet User accounts, see **User Manager on page 18**.

Menu Items

Introduction

Management Options

Both the Web and Control Console interfaces provide the capabilities that this section describes for managing the MasterSwitch PDU, but the information in this section is based on the Web interface. If you are using Telnet or a serial interface to access the MasterSwitch PDU, terminology may differ from what is used here.

Menu access depends on which type of account has logged on. See **Password-Protected Accounts on page 9** for more information on accounts.

Note: SNMP information appears in a separate document, ***Mibguide.pdf***, on this CD-ROM.

Menu Items

Outlets

Outlet Control Actions

You can perform the following Outlet Control Actions on individual outlets or on all accessible outlets as a group (by **Master Outlet Control)**. You can apply a Control Action only to an outlet that is not executing a command.

Item	Definition
Immediate On	The outlet turns on.
Immediate Off	The outlet turns off.
Immediate Reboot	The outlet turns off immediately, waits the outlet's Reboot Duration time, and turns on.
Delayed On	The outlet turns on according to its Power On Delay.
Delayed Off	The outlet turns off according to its Power Off Delay.
Sequenced Reboot	All outlets in the group assigned to the outlet user immediately turn off. Each outlet then waits the longest Reboot Duration (in seconds) of any outlet in the group, waits its own Power On Delay, and turns on.
Delayed Reboot	The outlet turns off after its Power Off Delay, waits its own Reboot Duration, and turns on.
Delayed Sequenced Reboot	Each outlet in the group of accessible outlets does the following: 1. Waits its own Power Off Delay. 2. Turns off. 3. Waits the longest Reboot Duration time (in seconds) of any outlet in the group. 4. Waits its own Power On Delay. 5. Turns on.
Cancel Pending Commands	All pending commands are canceled for the outlet(s). **Note:** The Outlet State appears in orange with an asterisk (*), indicating that a command is pending for the outlet(s).

Menu Items

MasterSwitch

Configure Device Settings

Item	Definition
Unit Name	The name of the MasterSwitch PDU. *Maximum:* 23 characters.
Coldstart Delay	The time that the MasterSwitch PDU waits before applying power to outlets after AC power is applied to the unit.
Reboot Duration	The longest reboot duration of any outlet in the group of accessible outlets. You can change this value only by modifying the Reboot Duration of individual accessible outlets. **Sequenced Reboot** and **Delayed Sequenced Reboot** use this value.

Outlet Configuration

Item	Definition
Outlet Name	The name that identifies the outlet. *Maximum:* 23 characters.
Power On Delay	The time that the outlet waits before turning on after the command is issued. **Delayed On**, **Sequenced Reboo**t, and **Delayed Sequenced Reboot** use this value.
Power Off Delay	The time that the outlet waits before turning off after the command is issued. **Delayed Off**, **Delayed Reboot**, and **Delayed Sequenced Reboot** use this value.
Reboot Duration	The time that the outlet will remain off during a reboot. **Immediate Reboot** and **Delayed Reboot** use this value.
URL Links	Defines HTTP links to relevant Web pages.

Menu Items

Event Log

Displaying the Event Log

To display the Event Log, select the **Event Log** menu in the Web interface or press CTRL + L in the Control Console interface.

The Event Log displays the following information for the most recent 300 events for the MasterSwitch PDU.

Item	Description
Date	The date on which the event occurred (*DD*/*MM*/*YYYY*)
Time	The time at which the event occurred (*HH*:*MM*:*SS*)
Event	Description of the event.

Retrieving the Event Log by using FTP

To retrieve the Event Log using client-side FTP:

1. From an MS-DOS prompt, type `ftp` *`card-ip`*, where *card-ip* is the IP address of your MasterSwitch PDU.
2. After you log into the unit's FTP server, type `dir`. The screen displays information similar to the following:

```
ftp>dir
200 Command okay.
150 Opening data connection for /.
--wx-wx-wx 1 apc apc 262144 Jul 5 2000 aos253.bin
--wx-wx-wx 1 apc apc 458752 Jul 5 2000 msp202.bin
-r--r--r-- 1 apc apc 4096 Jul 5 2000 event.txt
226 Closing data connection.
ftp: 194 bytes received in 0.00Seconds
194000.00Kbytes/sec.
ftp>
```

Continued on next page

Menu Items

Event Log *continued*

Retrieving the Event Log by using FTP, continued

3. Type `get event.txt`. The MasterSwitch PDU transmits the Event Log, containing at least the last 300 events, to your specified drive. The screen displays information similar to the following.

```
ftp>get event.txt
200 Command okay.
150 Opening data connection for event.txt
226 Closing data connection.
ftp: 3694 bytes received in 0.11Seconds
33.58Kbytes/sec.
ftp>
```

Using a spreadsheet to view the Event Log

To view the *event.txt* file after you obtain it, use a spreadsheet application. The file is TAB-delimited for automatic formatting of columns.

Note: When you import the *event.txt* file into a spreadsheet, the spreadsheet may display the year in the date fields as only two digits instead of the four digits logged and displayed by the MasterSwitch PDU. To display the year as four digits, select a four-digit date format in the spreadsheet.

The *event.txt* file also includes the following information that is not shown in the Web and Control Console Event Log screens:

- The version of the *event.txt* file format (first field).
- The date and time at which the *event.txt* file was retrieved.
- The Name, Contact, Location, and IP address for the unit's Management Card.
- A unique Event Code for every type of event.

Deleting the Event Log in the FTP interface

To delete the Event Log, type `del event.txt`. You are not prompted to confirm the deletion. The screen displays information similar to the following:

```
ftp>del event.txt
250 Requested file action okay, completed.
ftp>
```

A new *event.txt* file is created immediately in response to the Deleted Log event.

Menu Items

Network

TCP/IP

The **TCP/IP** section of the **Network** menu displays settings for the MasterSwitch PDU and allows you to configure the following TCP/IP settings.

Item	Description
System IP	The IP address of the MasterSwitch PDU
Subnet Mask	The network subnet mask
Default Gateway	The local default gateway (router address)
BOOTP	Enables or disables BOOTP requests for TCP/IP settings at startup.

TFTP/FTP

For control of file transfers, the **TFTP/FTP** section allows access to the following menu items on the **TFTP/FTP** menu for the TFTP and FTP Client and the FTP Server.

Client or Server	Menu Item	Definition
TFTP Client	**Remote Server IP:**	The network address of the TFTP server used for downloads.
FTP Client	**Remote Server IP:**	The network address of the FTP server used for downloads.
	User Name:	The user name for access to the FTP server.
	Password:	The password for access to the FTP server.
FTP Server	**Access:**	Enable or Disable FTP server access.
	Port:	The TCP/IP port on which the FTP server for the MasterSwitch PDU is located. *Default:* port 21

Continued on next page

Menu Items

Network *continued*

Telnet/Web

Port	Menu Item	Definition
Telnet	**Access**	Enables or Disables Telnet access.
	Port	The TCP/IP port where the Telnet server for the MasterSwitch PDU resides. *Default:* port 23
Web	**Access**	Enables or Disables Web access.
	Port	The TCP/IP port where the Web server for the MasterSwitch PDU resides. *Default:* port 80

SNMP

The **SNMP** section of the **Network** menu displays the following SNMP settings:

Item	Definition
SNMP Access	Enables or disables SNMP access.
Access Control	Controls access to each of the four SNMP channels.
Trap Receiver	Defines up to four network management stations (NMSs) to which traps are sent.

Continued on next page

Menu Items

Network *continued*

SNMP, continued

Access control. The **Access Control** section of the **SNMP** menu identifies the current settings for all four SNMP channels and provides the configurable values for a selected channel.

Item	Definition
Community Name	The password that the NMS (identified by the **NMS IP** option) must use for SNMP access to the MasterSwitch PDU. The allowed access type is defined by the **Access Type** option. Maximum: 15 characters.
NMS IP	Limits access to the NMS or NMSs specified. You specify the value as a specific IP address for one NMS or as an IP address filter for multiple IP addresses. For example: • **159.215.12.1** allows only the NMS with the specific IP address of 159.215.12.1 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.
Access Type	Defines what actions the NMS that is identified by the **NMS IP** option can perform: • Write: The NMS can use GETs and SETs. • Read: The NMS can use only GETs. • Disabled: The NMS can use neither GETs nor SETs.

Trap Receiver. The **Trap Receiver** section of the **SNMP** menu identifies the current settings for all four trap receivers and allows you to change the values for a selected trap receiver.

Item	Definition
Community Name	The password that the MasterSwitch PDU uses when it sends traps to the NMS identified by the Receiver NMS IP option. *Maximum:* 15 characters.
Receiver NMS IP	The IP address of the NMS that will receive traps sent by the MasterSwitch PDU. **Note:** To send no traps to any NMS, set 0.0.0.0 as the Trap Receiver IP.
Trap Generation	Enables or Disables the ability of the MasterSwitch PDU to send traps to the NMS identified by the **Receiver NMS IP** option.
Authentication Traps	Enables or Disables the ability of the MasterSwitch PDU to send authentication traps to the NMS identified by the **Receiver NMS IP** option.

Menu Items

System

User Manager

The **User Manage**r section of the **System** menu displays the following configurable properties of the Administrator and Device Manager accounts.

Administrator Account	
Item	**Definition**
Auto Logout	The amount of time the user can be inactive on the system before being logged out automatically. *Default:* 3 minutes.
Authentication	One of the following settings: • Basic: Causes the Web Interface to use standard HTTP 1.1 login (base64-encoded passwords). • MD5: Causes the Web Interface to use an MD5-based authentication login. For MD5 authentication to function properly, you must have cookies enabled in your browser. *Default:* Basic
User Name	The user name. *Access:* Administrator only *Maximum:* 10 characters *Default:* apc
Password	The password for HTTP 1.1 authentication only Access: Administrator only *Maximum:* 10 characters *Default:* apc
Authentication Phrase	The password for MD5 only. *Access:* Administrator only *Minimum:* 15 characters *Maximum:* 32 characters *Default:* admin user phrase

Continued on next page

Menu Items

System *continued*

User Manager, continued

Device Manager Account	
Item	**Definition**
User Name	The user name. *Maximum:* 10 characters *Default:* device
Password	The password for HTTP 1.1 authentication only. *Maximum: 10 characters* *Default*: apc
Authentication Phrase	The password for MD5 only. *Minimum:* 15 characters *Maximum:*32 characters *Default:* device user phrase

Continued on next page

Menu Items

System *continued*

Outlet User Management

You can create up to 16 independent Outlet User accounts for a MasterSwitch PDU.

Current Outlet User List. The list shows the existing outlet user accounts and the outlets to which they have access. To select an existing account to edit or delete, click on the underlined user name, To add a user, select **Add New User**.

Configure the Outlet User Account Settings. Following are the configurable settings for Outlet User Manager.

Item	Definition
User Name	The outlet user name for both HTTP 1.1 and MD5 authentication. *Maximum*: 10 characters **Note:** If the User Name is in orange, the user account has been disabled.
Password	The outlet user password for HTTP 1.1 authentication. *Maximum*: 10 characters
Authentication Phrase	The Outlet user authentication phrase for MD5. *Minimum*: 15 characters *Maximum*: 32 characters.
User Description	A descriptive Identification of the outlet user. *Maximum*: 30 characters
Account Status	Enables, disables, or deletes the outlet user's account. **Note**: A disabled account prevents the Outlet User of the account from logging in. The User Name is in orange if the account has been disabled.
MasterSwitch Outlet Access	Selects the specific outlets to which an outlet user will have access.
Delete User	To delete an account, change the Account status to delete Outlet User, or click **Delete User**.

Continued on next page

Menu Items

System *continued*

Identification

Item	Definition
Name	The system name used to identify the device. Name will be used for the ***sysName*** OID in the SNMP agent.
Contact	The contact for or owner of the device. Contact will be used for the ***sysContact*** OID in the SNMP agent.
Location	The physical location of the device. Location will be used for the ***sysLocation*** OID in the SNMP agent.

Date/Time

Item	Definition
Date	The date for the system in the following format: *MM*/*DD*/*YY*.
Time	The time for the system in the following format: *HH*:*MM*:*SS* (24-hour time).

Continued on next page

Menu Items

System *continued*

File Transfer

The **File Transfer** section of the **System** menu provides access for managing file transfers.

Item	Description
Remote TFTP Server IP	The IP address of the remote TFTP server defined in the **Network** menu's TFTP/FTP settings. *TFTP:* Remote Server IP
Remote FTP Server IP	The IP address of the remote FTP server defined in the **Network** menu's TFTP/FTP settings. *FTP:* Remote Server IP
Remote FTP Server User Name	The user name for the FTP server defined in the **Network** menu's TFTP/FTP settings. *FTP Client:* User Name
Remote FTP Server Password	The password for the FTP server defined in the **Network** menu's TFTP/FTP settings. *FTP Client:* Password
Filename	The name of the file to be downloaded.
Result of Last File Transfer	Displays the results of the last file transfer.
Initiate File Transfer Via	Lets you choose whether the file will be transferred by TFTP or FTP.

Continued on next page

Menu Items

System *continued*

Tools

Item	Definition
No Action	Causes no action.
Reboot Card	Restarts the operation of the Management Card, but does not affect the state of the MasterSwitch outlets.
Reset Card to Defaults	Restores all configuration settings, including TCP/IP settings and user accounts, to their defaults and enables BOOTP.
Reset Card to Defaults Except TCP/IP	Restores all configuration settings to the default except TCP/IP settings.

Links

The link names that you configure appear on the navigation menu at the left in the Web interface. (The APC links are pre-defined but can be changed.)

Link Type	Item	Definition
User Links	**Name**	A link name that will appear on the menu bar. Up to 3 are allowed.
	URL	The HTTP link in URL form for the link name specified as Name: `http://mysite.com/mypage.com`
APC Links	**Name**	View the names of the APC links.
	URL	Define the URL of each APC link.

Note: Only the Web interface of the MasterSwitch PDU displays hyperlinks and allows you to define them.

Menu Items

Help

Contents

The **Contents** screen provides an overview of many parameters reported and configured through the Web and Control Console interfaces.

Accessing and Navigating the Online Help

To access the online help, do one of the following:

- In the Web interface, select **Help** at the lower left in the navigation frame.
- In the Control Console, type `?` to access the **Help** menu.

When using any menu, you can access the internal help pages by clicking **?** at the end of the black title bar

APC Interactive Assistant

APC Interactive Assistant brings APC Customer Service to the Web. When you select APC Interactive Assistant, the MasterSwitch PDU transmits information to the APC Interactive Assistant server. The server then provides customized up-to-date product information (such as whether a later version of firmware is available) and provides access to extensive context-sensitive help.

About Card

About Card provides the following information about the MasterSwitch PDU:

- The serial number
- The hardware revision
- The date and time at which the application version and APC OS information was loaded.

Configuring and Using E-mail Notification

Configuring E-mail Recipients

Menu options

To identify up to four e-mail recipients, use one of the following:

- The **Recipients** option of the Web interface's **Events** menu
- The **E-mail** option of the Control Console's **Network** Menu

Settings

Setting	Description
To Address	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway generates the page. **Note:** The recipient's pager must be able to use text-based messaging.
Send via	Lets you choose one of the following methods for routing e-mail: • Send e-mail through the Management Card's SMTP server. Selecting **Local SMTP Server**, which is the recommended option, ensures that the e-mail is sent before the unit's 20-second time-out, and, if necessary, is retried several times. • Send e-mail directly to the recipient's remote SMTP server. If you select the **Recipient's SMTP Server** option, and the remote SMTP server is busy, the time-out may prevent some e-mail from being sent, With this option, the management card tries to send the e-mail only once.
E-mail Generation	Enables (by default) or disables sending e-mail to the defined recipient.

Configuring the local SMTP server

When you select the **Local SMTP Server** option for the **Send via** setting, you must do one of the following:

- Make sure that forwarding is enabled at that server so that the server can route e-mail to external SMTP servers.

  Note: Always see your SMTP-server administrator before changing the configuration of your SMTP server.
- Set up a special e-mail account for the Management Card. This account then forwards the E-mail to an external e-mail account.

Testing E-mail

In the Web interface, use the **E-mail Test** option to send a test e-mail message to a configured recipient.

Configuring and Using E-mail Notification

Configuring SMTP and DNS Settings

Requirements for using SMTP

To use the Simple Mail Transfer Protocol (SMTP) to send e-mail when an event occurs, you must define the following settings:

- The IP address of the Domain Name Service (DNS) server.
- The DNS name of the SMTP server and the **From Address** settings for SMTP.
- The e-mail addresses for a maximum of four recipients.

Note: To page an e-mail recipient who uses a text-based pager gateway, see the description of the **To Address** setting in **Settings on page 25**.

DNS server

To enable the Management Card to send e-mail messages, you must use the **TCP/IP & DNS** option (Web interface) or **DNS** option (Control Console) in the **Network** menu to identify the Domain Name Service (DNS) server by its IP address.

If the unit does not receive a response from the DNS server within five seconds, e-mail cannot be sent. Therefore, use a DNS server on the same segment as the unit or on a nearby segment (but not across a WAN).

After you define the DNS server's IP address, verify that DNS is working correctly by entering the DNS name of a computer on your network to obtain the IP address for that DNS name.

SMTP settings

The **E-mail** option in the **Network** menu accesses the following SMTP settings:

Setting	Description
SMTP Server	The DNS name of the SMTP server.
From Address	The contents of the **From** field in the e-mail messages sent by the Management Card. **Note:** See the documentation for your SMTP server to determine whether you must use a valid user account on the server for this setting.

Event-Related Menus and Options

Event Log

Logged events

The Management Card's event log records normal and abnormal Management Card (system) events and MasterSwitch events. Any conditions that cause an SNMP trap, except for SNMP authentication failures, are logged as events. For a list of all events, see **Management Card and MasterSwitch Events on page 36**.

To disable the logging of events based on their assigned severity level, use the **Actions** option in the Web interface's **Events** menu, as described on **page 29**.

Accessing the log

To view or clear the Management Card's event log, use the Web interface, control console, or FTP.

Web interface. To display the last 300 (or fewer) events recorded in the event log, in reverse chronological order, use the **Log** option in the **Events** menu.

To clear all events from the log, use the **Delete Log** button.

Control Console. Use the control console from a local computer (by direct serial-cable connection) or over the network (using Telnet) to do the following:

- To display the event log, in reverse chronological order, press CTRL+L.
- To scroll through the last 300 (or fewer) recorded events, use the space bar.
- To clear all events from the log, type `d` and press ENTER while viewing the log.

Continued on next page

Event-Related Menus and Options

Event Log *continued*

Accessing the log, continued

FTP. The **event.txt** file is a text version of the Management Card's event log.

- It is tab-delimited so that it can be imported into any spreadsheet application.
- It reports as many as 5000 events that occurred since the log was last deleted.
- It includes information that is not displayed in the Management Card's event log as displayed by the Web interface and control console.
  - The version of the **event.txt** file format (first field).
  - The **Date** and **Time** the **event.txt** file was retrieved.

    Note: You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.
  - The **Name**, **Contact**, **Location**, and IP address of the Management Card.
  - The unique **Event Code** for every type of event.

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

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

   ```
   ftp 159.215.12.114
   ```

2. Log on.

   Note: Case-sensitive **User Name** and **Password** settings (**apc** by default for both) protect FTP access. On the **Network** menu, use the **FTP** option in the control console or the **TFTP & FTP** option in the Web interface to change these settings.

3. Use the `get` command to transmit the text-version of the Management Card's event log to your local drive.

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

To clear all events from the log, use the `del` command. A new **event.txt** file is created immediately to record the Deleted Log event.

```
ftp>del event.txt
250 Requested file action okay, completed.
ftp>
```

To exit from FTP, type `quit`.

Event-Related Menus and Options

Actions Option (Web Interface only)

Enabling and disabling event actions

Use the **Actions** option of the **Events** menu to enable or disable the following for events that have a specified severity level:

- **Events Log**
- **SNMP Traps**
- **Email**

Some Management Card (system) events do not have a severity level, and you cannot disable actions for those events.

Severity levels of events

All MasterSwitch events and some Management Card events have a default severity level of Severe, Warning, or Informational. See **Severity levels defined on page 36**.

To use an **evntlist.htm** page to change the default severity level of an event, see **How to Configure Individual Events on page 33**.

Event Log action

Disable this action to prevent the logging of all events that have a severity level. By default, all events are logged.

SNMP Traps action

By default, the **SNMP Traps** action is enabled for all MasterSwitch events and for Management Card events that have a severity level (informational, warning, or severe).

To use SNMP traps for event notifications, you must first identify the trap receivers (up to four) by their specific IP addresses. See **Trap receivers on page 30**.

Email action

By default, the **Email** action is enabled for severe events only. To use e-mail for event notification, you must first define the e-mail recipients. See **page 31**.

Related topics

See **Event Log on page 27**.

See **Management card events on page 37** and **MasterSwitch events on page 38** for a description and the default severity level (if any) for each event.

Event-Related Menus and Options

Recipients Option

Trap receivers

You can define up to four NMSs to be used as trap receivers when an event occurs that has SNMP traps enabled.

In the Web interface, use the **Trap Receiver** settings, available through the **Recipients** option of the **Events** menu.

In the control console, use the **SNMP** option of the **Network** menu.

Item	Definition
Community Name	The password (15 characters or less) used when traps are sent to the NMS identified by the **Receiver NMS IP** setting.
Receiver NMS IP	The IP address of the NMS to which traps are sent. If this setting is **0.0.0.0** (the default), no traps are sent to any NMS.
Trap Generation	Enables (by default) or disables the sending of any traps to the NMS identified by the **Receiver NMS IP** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP** setting.

Continued on next page

Event-Related Menus and Options

Recipients Option *continued*

Email Recipients

To identify up to four e-mail recipients to be notified of events, use one of the following:

- The **Recipients** option of the Web interface's **Events** menu
- The **Email** option of the control console's **Network** Menu

Setting	Description
To Address	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway pages the recipient. **Note:** The recipient's pager must be able to use text-based messaging.
Send via	Selects one of the following methods for routing e-mail: • Through the Management Card's SMTP server (the recommended option, **Local SMTP Server**). This option ensures that the e-mail is sent before the Management Card's 20-second timeout, and, if necessary, is retried several times. • Directly to the recipient's SMTP server (the **Recipient's SMTP Server** option). On a busy remote SMTP server, the timeout may prevent some e-mail from being sent, and with this option, the Management Card tries to send the e-mail only once. When the recipient uses the Management Card's SMTP server, this setting has no effect.
Email Generation	Enables (by default) or disables sending e-mail to the defined recipient.

When you select the **Local SNMP Server** option for the **Send via** setting, you must do one of the following:

- Make sure that forwarding is enabled at that server so that the server can route e-mail to external SMTP servers.

  Note: Always see your SMTP server's administrator before changing the configuration of your SMTP server.
- Set up a special e-mail account for the Management Card. This account then forwards the e-mail to an external account.

In the Web interface, use the **Email Test** option to send a test message to a configured recipient.

Event-Related Menus and Options

Email Option

Requirements for using SMTP

To use the Simple Mail Transfer Protocol (SMTP) to send e-mail when an event occurs, you must define the following settings:

- The IP address of the domain name service (DNS) server.
- The DNS name of the SMTP server and the **From Address** settings for SMTP.
- The e-mail addresses for a maximum of four recipients.

  Note: To page an e-mail recipient who uses a text-based pager gateway, see the description of the **To Address** setting in **Email Recipients on page 31**.

DNS server

To enable the Management Card to send e-mail messages, you must use the **TCP/IP & DNS** option (Web interface) or **DNS** option (control console) in the **Network** menu to identify the domain name service (DNS) server by its IP address.

If the Management Card does not receive a response from the DNS server within five seconds, e-mail cannot be sent. Therefore, use a DNS server on the same segment as the Management Card or on a nearby segment (but not across a WAN).

After you define the DNS server's IP address, verify that DNS is working correctly by entering the DNS name of a computer on your network to obtain the IP address for that DNS name.

SMTP settings

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

Setting	Description
SMTP Server	The DNS name of the SMTP server.
From Address	The contents of the **From** field in the e-mail messages sent by the Management Card. **Note:** See the documentation for your SMTP server to determine whether you must you use a valid user account on the server for this setting.

Event-Related Menus and Options

How to Configure Individual Events

Options to configure individual events

You can configure individual events as follows:

- Use the **evntlist.htm** page. See **Event list access on this page**.
- Use the I2C Configuration Utility on the MasterSwitch CD. You edit a text file (.ini file,) convert that file to a binary configuration file (.cfg file), and use the Management Card Wizard to send the .cfg file to multiple Management Cards over the network. See the *Management Card Addendum* on the MasterSwitch CD.

To configure the actions for events based on their default severity levels instead of individually, see **Actions Option (Web Interface only) on page 29**.

Event list access

To access the event list, add **/evntlist.htm** to the Management Card's URL address value (IP address or DNS name). You cannot access the event list directly from the Web interface menus.

- For an IP address of 159.215.12.114, and the default TCP port of 80, the URL is:
  `http://159.215.12.114/evntlist.htm`
- For an IP address of 159.215.12.114, and a TCP port other than 80 (in this example, 5000), the URL is:
  `http://159.215.12.114:5000/evntlist.htm`
- For a DNS name of `writers`, the URL is:
  `http://writers/evntlist.htm`

Event list format

The **evntlist.htm** page defines the following for each event:

- **Code:** The event's unique event code.
- **Description**: The text used for the event.
- **Severity**: The event's default severity level.
- **Configuration**: The hexadecimal code that defines the actions to occur for the event and provides a link to the event mask that you use to configure the event. See **Event mask settings on page 34**.

Continued on next page

Event-Related Menus and Options

How to Configure Individual Events *continued*

Event mask settings

From the **evntlist.htm** page, to reconfigure actions for an event:

1. Click the link (the current hexadecimal code) for the event.
2. Enter a new hexadecimal code as an event mask to reconfigure the bits that control the actions for the event
3. Click **Apply**.

The bits are numbered 0 to 23, from left to right.

Note: Bit 5 and bits 14 through 23 are unused. Make sure these bits are always set to 0.

Bits 0 to 3 represent the event's severity:

Settings for Bits 0 to 3	Severity
0000	No severity
0001	Informational
0010	Warning
0011	Severe

Bit 4 and bits 6 to 9 enable (1) or disable (0) event logging. and trap receivers for the event:

Bit number	Action enabled or disabled for the event
4	Logging the event.
6	Sending traps to Trap Receiver 1
7	Sending traps to Trap Receiver 2
8	Sending traps to Trap Receiver 3
9	Sending traps to Trap Receiver 4

Bits 10 to 13 enable (1) or disable (0) e-mail recipients for the event:

Bit number	Action enabled or disabled for the event
10	Sending e-mail to recipient 1
11	Sending e-mail to recipient 2
12	Sending e-mail to recipient 3
13	Sending e-mail to recipient 4

Continued on next page

Event-Related Menus and Options

How to Configure Individual Events *continued*

Event mask example

You enter the hexadecimal code 3B0800 as an event mask.

The event mask configures the following bit settings:

```
0011 1011 0000 1000 0000 0000
```

The event is configured as follows:

- The severity level is severe.
- The event will be logged.
- Traps generated by the event will be sent to trap receivers 1 and 2.
- When the event occurs, e-mail will be sent to recipient 3 only.

Event-Related Menus and Options

Management Card and MasterSwitch Events

Event generation

The Management Card and MasterSwitch both generate events, which are logged in the event log.

Any event of either type generates a unique code, which you can use in applications to identify the event.

To use SNMP traps for event notifications, you must first identify the trap receivers (up to four) by their specific IP addresses. See **Trap receivers on page 30**.

Severity levels defined

Severity	Definition
Severe	Requires immediate action. Severe events can cause incorrect operation of the DC Power Plant or its supported equipment or can cause loss of power protection during a power failure.
Warning	Needs action if the condition worsens, but does not require immediate attention.
Informational	Requires no action.

Note: All MasterSwitch events and some Management Card events have a severity level.

For information about how severity levels define the actions associated with events, see **Actions Option (Web Interface only) on page 29**.

Continued on next page

Event-Related Menus and Options

Management Card and MasterSwitch Events *continued*

Management card events

Code	Severity	Description
0x0001	Severe	System: Coldstart. (The Management Card was turned on.)
0x0002	Severe	System: Warmstart. (The Management Card was reset after it was already turned on.)
0x0003	Warning	System: SNMP configuration change.
0x0004	Informational	System: An unauthorized user attempted to access the SNMP interface.
0x0005	Warning	System: An unauthorized user attempted to access the control console interface.
0x0006	Warning	System: An unauthorized user attempted to access the Web interface.
0x0008	Warning	System: Password changed.
0x000C	No severity	System: File transfer started. (FTP)
0x000D	No severity	System: File transfer started. (TFTP)
0x000F	No severity	System: File transfer failed.
0x0014	No severity	System: Control console user logged on.
0x0015	No severity	System: Web user logged on.
0x0016	No severity	System: FTP user logged on.
0x0018	No severity	System: Reset to Defaults.
0x0019	No severity	System: Initializing data.

Note: You cannot configure actions for Management Card events that have no severity level.

Continued on next page

Event-Related Menus and Options

Management Card and MasterSwitch Events *continued*

MasterSwitch events

Code	Severity	Description
0x0501	Warning	An outlet has rebooted. If the outlet number is 0, then all outlets have rebooted.
0x0509	Warning	An outlet has turned on. If the outlet number is 0, then all outlets have turned on.
0x050B	Warning	An outlet has turned off. If the outlet number is 0, then all outlets have turned off.
0x0510	Warning	An outlet has changed configuration. If the outlet number is 0, then the Master outlet has changed.
0x0901	Informational	Add user.
0x0902	Informational	Delete user.
0x0903	Informational	Edit user.

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the MasterSwitch PDU 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.

Port assignments

If a Telnet, FTP, or Web 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 the Telnet, FTP, and Web servers listen are initially set at the standard “well known ports” for the protocols.To hide the interfaces, use any port numbers from 5000 to 65535.

User names, passwords, community names

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 in to the Administrator, Device Manager, and Outlet User accounts of the Control Console or Web interface of a MasterSwitch PDU. This security limitation of the protocols affects any device using Telnet, a Web server, or an SNMP version 1 agent.

Security

Authentication

Authentication versus encryption

The MasterSwitch PDU controls access by providing basic authentication through user names, passwords, and IP addresses, but provides no type of encryption. These basic security features are sufficient for most environments, in which sensitive data is not being transferred. To ensure that data and communication between the MasterSwitch PDU and the client interfaces, such as Telnet and the Web browser, cannot be captured, you can provide a greater level of security by enabling MD5 authentication (described below) for the Web interface.

MD5 authentication (Web interface)

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

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

Continued on next page

Security

Authentication *continued*

MD5 authentication (Web interface), continued

If you use MD5 authentication, which is available only for the Web interface, disable the less secure interfaces, including Telnet, FTP, and SNMP. For SNMP, you can disable write-only access so that read access and trap facilities are still available.

Although MD5 authentication provides a much higher level of security than the plain-text access methods, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme. For additional information on MD5 authentication, see RFC document #1321 at the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

Continued on next page

Security

Authentication *continued*

Summary of access methods

Interface	Security Access	Notes
Serial Control Console	Access is by user name and password.	Always enabled.
Telnet Control Console	These methods are available: • User name and password • Selectable server port • Server Enable/Disable	The user name and password are transmitted as plain text.
SNMP	These methods are available: • Community Name • NMS IP filters • Agent Enable/Disable • Four access communities with read/write/disable capability	NMS IP filters allow access from either one IP address or from multiple IP addresses. You specify multiple NMSs not by their literal IP addresses but in the format of an NMS IP filter. See **Access control on page 17** for more information.
FTP Server	These methods are available: • User name and password • Selectable server port • Server Enable/Disable	Only the Administrator account has access.
Web Server	These methods are available: • User name and password • Selectable server port • Server Enable/Disable • MD5 Authentication option	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase.

Product Information

Warranty Information

Limited warranty

American Power Conversion (APC) warrants the MasterSwitch PDU 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.

Obtaining service

To obtain service under warranty, you must obtain a Returned Material Authorization (RMA) number from APC or a designated APC service center. Products must be returned to APC or to an APC service center with transportation charges prepaid and must be accompanied by a brief description of the problem and proof of date and place of purchase. See **Contacting Customer Support on page 44** for more information, including packaging, shipping, and labeling requirements for returned products.

Warranty exclusions

Except as provided herein, American Power Conversion makes no warranties, express 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 from state to state.

Product Information

Obtaining Customer Support

Contacting Customer Support

To obtain customer support for problems with the MasterSwitch PDU:

1. Contact Customer Support at a phone number or address listed under **APC Worldwide Customer Support on page 53**, and be ready to provide the serial number and date of purchase of the MasterSwitch PDU.
2. Be prepared to provide a description of the problem so that the technician can attempt to solve the problem over the phone.
3. If phone consultation cannot solve the problem, the technician will give you a Return Material Authorization (RMA) number. If the MasterSwitch PDU is under warranty, repair or replacement is free of charge. If the warranty has expired, there will be a charge for repair or replacement.
4. If you are asked to return the MasterSwitch PDU, pack the unit carefully. Damage sustained in transit is not covered by the warranty.
   - Enclose a letter in the package with your name, address, RMA number, a copy of the sales receipt, your daytime phone number, and a check as payment (if applicable).
   - Mark the RMA number clearly on the outside of the shipping carton. The factory will not accept any materials without this marking.
5. Return the MasterSwitch PDU by insured, prepaid carrier to the address provided by the technician.

Product Information

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 or 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.

Product Information

Specifications

Product specifications for AP9211

Type of Specification	Item	Specification
Electrical	Input: Nominal input voltage Acceptable input voltage Nominal input frequency Overcurrent protection Input connector	 100–120 VAC 90–140 VAC 50/60 Hz 15-A circuit breaker 15 ft (4.5 m) attached NEMA 5-15 line cord
	Output: Output connectors	 Eight NEMA 5-15 outlets
	Maximum total current draw:	12 A
Physical	Size (H × W × D)	1.75 × 17.0 × 6.5 in (4.4× 43.2 × 16.5 cm)
	Weight:	6.0 lb (2.7 kg)
	Shipping weight:	7.5 lb (3.4 kg)
Environmental	Elevation (above MSL): Operating Storage	 0 to 10,000 ft (0 to 3000 m) 0 to 50,000 ft (0 to 15 000 m)
	Temperature: Operating Storage	 32 to 104°F (0 to 40°C) 32 to 113°F (0 to 45°C)
	Operating Humidity:	0 to 95%, non-condensing
Approvals	EMC verification:	FCC Class A; DOC Class A; VCCI
	Safety Agency:	CSA; UL

Continued on next page

Product Information

Specifications *continued*

Product specifications for AP9212

Type of Specification	Item	Specification
Electrical	Input: Nominal input voltage Acceptable input voltage Nominal input frequency Overcurrent protection Input connector	 100-230 VAC 90-250 VAC 50/60 Hz 12-A circuit breaker IEC-320 C14 inlet and IEC-320 C13-to-C14 power extender cord (2m)
	Output: Output connectors	 Eight IEC-320 C13 outlets
	Maximum total current draw:	10 A
Physical	Size (H × W × D)	1.75 × 17.0 × 6.5 in (4.4× 43.2 × 16.5 cm)
	Weight:	4.5 lb (2.0 kg)
	Shipping weight:	6.0 lb (2.7 kg)
Environmental	Elevation (above MSL): Operating Storage	 0 to 10,000 ft (0 to 3000 m) 0 to 50,000 ft (0 to 15 000 m)
	Temperature: Operating Storage	 32 to 104°F (0 to 40°C) 32 to 113°F (0 to 45°C)
	Operating Humidity:	0 to 95%, non-condensing
Approvals	EMC verification:	CE with CISPR 22 and 24
	Safety Agency:	VDE; IEC 60950

Continued on next page

Product Information

Specifications *continued*

Product specifications for AP9217

Type of Specification	Item	Specification
Electrical	Input: Nominal input voltage Acceptable input voltage Nominal input frequency Overcurrent protection Input connector	 100–120 VAC 90–140 VAC 50/60 Hz 20-A circuit breaker 12 ft (3.7 m) attached, NEMA L5-20, twist lock cord
	Output: Output connectors	 Eight NEMA 5-15 outlets
	Maximum total current draw:	16A
Physical	Size (H × W × D)	1.75 × 17.0 × 6.5 in (4.4× 43.2 × 16.5 cm)
	Weight:	6.6 lb (3.0 kg)
	Shipping weight:	9.0 lb (4.1 kg)
Environmental	Elevation (above MSL): Operating Storage	 0 to 10,000 ft (0 to 3000 m) 0 to 50,000 ft (0 to 15 000 m)
	Temperature: Operating Storage	 32 to 104°F (0 to 40°C) 32 to 113°F (0 to 45°C)
	Operating Humidity:	0 to 95%, non-condensing
Approvals	EMC verification:	FCC Class A; DOC Class A; VCCI
	Safety Agency:	UL

Continued on next page

Product Information

Specifications *continued*

Product specifications for AP9218

Type of Specification	Item	Specification
Electrical	Input: Nominal input voltage Acceptable input voltage Nominal input frequency Overcurrent protection Input connector	 100-230 VAC 90-250 VAC 50/60 Hz 20-A circuit breaker IEC-320 C20 inlet and IEC-320 8.2 ft (2.5 m), detached, IEC C20-H05W-F361, 50-C-19 cord
	Output: Output connectors	 Eight IEC 320-C13 outlets
	Maximum total current draw:	16 A
Physical	Size (H × W × D)	1.75 × 17.0 × 6.5 in (4.4× 43.2 × 16.5 cm)
	Weight:	6.6 lb (3.0 kg)
	Shipping weight:	9.0 lb (4.1 kg)
Environmental	Elevation (above MSL): Operating Storage	 0 to 10,000 ft (0 to 3000 m) 0 to 50,000 ft (0 to 15 000 m)
	Temperature: Operating Storage	 32 to 104°F (0 to 40°C) 5 to 149°F (-15 to 65°C)
	Operating Humidity:	0 to 95%, non-condensing
Approvals	EMC verification:	CE with CISPR 22 and CISPR24 FCC Part 15 Class A, AS/NZS 3548 and VCCI
	Safety Agency:	VDE; IEC 60950, UL

Index

Index

Index

APC Contact Information

APC Worldwide Customer Support

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

- Use an APC web page to find answers to frequently asked questions (FAQs), to access documents in the APC Knowledge Base, and to submit customer support requests.
  - **http://www.apcc.com** (Corporate Headquarters)
    Connect by links to APC web pages for specific countries and regions, each of which provides customer support information.
  - **http://www.apcc.com/support/**
    Submit customer support requests.
- Contact local or regional APC Customer Support by telephone or e-mail.
  - For e-mail addresses and local, country-specific, customer support telephone numbers worldwide, go to **http://www.apcc.com/support/contact**.
  - For e-mail addresses and technical support telephone numbers of major APC regional customer support centers, use the following list:

APC Headquarters (U.S. and Canada)	(1) (800) 800-4272 (toll free)
Latin America	(1) (401) 789-5735 (United States) apctchla@apcc.com
Europe, Middle East, Africa	(353) (91) 702020 (Ireland) apceurtech@apcc.com
Japan	(03) 5434-2021 jsupport@apcc.com

- Contact the APC representative or other distributor from whom you purchased your APC hardware device or APC software application for information on how to obtain local customer support.

990-6018E **07/2001**