Schneider Electric
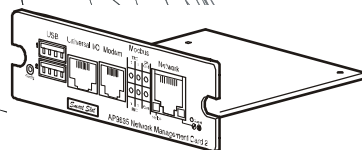
Installation Manual

Network Management Card

AP9635

This manual is available in English on the enclosed CD.

Dieses Handbuch ist in Deutsch auf der beiliegenden CD-ROM verfügbar.

Este manual está disponible en español en el CD-ROM adjunto.

Ce manuel est disponible en français sur le CD-ROM ci-inclus.

Questo manuale è disponibile in italiano nel CD-ROM allegato.

本マニュアルの日本語版は同梱の CD-ROM からご覧になれます。

O manual em Português está disponível no CD-ROM em anexo.

Данное руководство на русском языке имеется на прилагаемом компакт-диске.

您可以从包含的 CD 上获得本手册的中文版本。

동봉된 CD 안에 한국어 매뉴얼이 있습니다 .

Contents

Preliminary Information

Features

The American Power Conversion Network Management Card has standard features that do the following:

- Detect 10/100 Mbps connection speeds
- Provide a data log accessible by File Transfer Protocol (FTP), Secure CoPy (SCP), or a Web browser
- Provide an event log that is accessible by Telnet, Secure SHell (SSH), FTP, SCP, or a Web browser
- Generate system log (Syslog) messages
- Enable you to configure a BOOTstrap Protocol (BOOTP) or Dynamic Host Configuration Protocol (DHCP) server to provide the TCP/IP values a Network Management Card needs for network communication
- Generate e-mail notifications for UPS or system events
- Limit SNMP traps, e-mail notification, and event logging based on severity and categories of events
- Enable you to configure multiple Network Management Cards simultaneously over the network
- Provide enhanced security by supporting SSH, Secure Sockets Layer (SSL) and Secure CoPy (SCP)
- Support external environmental sensors (part numbers AP9810, AP9335T, and AP9335TH)
- Support Modbus RTS via a RS-485 connection.
- Support Remote Monitoring over modem with TLS (MGE Galaxy models only)

Related documents

The Network Management Card *Utility* CD contains the following documentation:

- *Network Management Card User's Guide*
- *Network Management Card Upgrade Utilities*
- *Security Handbook*
- *PowerNet® Management Information Base (*MIB) *Reference Guide*

Inventory

The Network Management Card package includes the following items:

- This *Installation Manual*
- Network Management Card
- Network Management Card *Utility* CD
- Serial configuration cable (940-0299)
- Temperature sensor (AP9335T)—AP9631 Network Management Card only
- Network Management Card quality assurance test slip
- Declaration of Conformity
- Warranty registration form
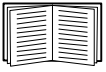
Save the quality assurance test slip. The slip contains the MAC address that you may need when performing the procedures in "TCP/IP configuration methods" on page 4.

Disclaimer

American Power Conversion is not responsible for damage sustained during reshipment of this product.

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

Please recycle

The shipping materials are recyclable. Save them for later use, or dispose of them appropriately.

Management products, including the Network Management Card, contain removable, lithium coin-cell batteries. When discarding these batteries, you must follow local rules for recycling.

Installation in a Symmetra PX or Galaxy UPS

You do not need to turn off the power for an MGE Galaxy, Symmetra PX 250 or Symmetra PX 500 UPS before you remove or install the Management Card.

The Network Management Card is sensitive to static electricity. When handling the Management Card, touch only the end plate while using one or more of these electrostatic-discharge devices (ESDs): wrist straps, heel straps, toe straps, or conductive shoes.
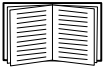
For the location of the UPS card slot, see the UPS documentation.

1. Locate the UPS card slot.
2. Use the same screws that hold the slot cover in place to secure the Management Card in the UPS card slot.
3. Connect a network interface cable to the 10/100Base-T network connector ❶ on the Management Card.
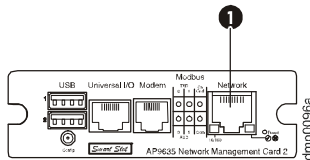
Quick Configuration

Overview

Note: Disregard the procedures described in this chapter if you have InfraStruXure® Central as part of your system. See the documentation for your InfraStruXure device for more information.

You must configure the following TCP/IP settings before the UPS Network Management Card (NMC) can operate on a network:

- IP address of the NMC
- Subnet mask
- Default gateway

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

Caution: Do not use the loopback address (127.0.0.1) as the default gateway address for the NMC. It disables the card and requires you to reset TCP/IP settings to their defaults using a local serial login.
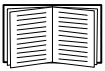
See "Watchdog Features" in the "Introduction" of the NMC *User's Guide* for more information about the watchdog role of the default gateway.

TCP/IP configuration methods

Use one of the following methods to define the TCP/IP settings needed by the Network Management Card:

- Device IP Configuration Wizard (See "Device IP Configuration Wizard" on page 5.)
- BOOTP or DHCP server (See "BOOTP and DHCP configuration" on page 5.)
- Networked computer (See "Local access to the command line interface" on page 8 or "Remote access to the command line interface" on page 8.)
- The UPS user interface display (See "User interface display" on page 10.)

Device IP Configuration Wizard

You can use the Device IP Configuration Wizard at a computer running
Microsoft® Windows® 2000, Windows Server® 2003, Windows XP, Windows
Vista, Windows Server 2008, or Windows 7 to discover unconfigured Network
Management Cards and configure their basic TCP/IP settings, one card at a
time, over the network.

> **Note:** Most software firewalls must be temporarily disabled for the
> Wizard to discover unconfigured Network Management Cards.

1. If autorun is enabled, the user interface of the CD starts when you
   insert the Network Management Card *Utility* CD into a computer on
   your network. Otherwise, open the file **contents.htm** on the CD.

2. Select the Device IP Configuration Wizard from the main menu.

3. When the Wizard discovers the unconfigured Network Management
   Card, follow the on-screen instructions.

> **Note:** If you leave the option **Start a Web browser when finished**
> enabled, you can access the Network Management Card through
> your browser by using **apc** (the default) for both the user name and
> password.

.ini file utility

You can use the .ini file export utility to export .ini file settings from configured
Network Management Cards to one or more unconfigured Network
Management Cards. The utility and documentation are included on the Network
Management Card *Utility* CD.

BOOTP and DHCP configuration

The default TCP/IP configuration setting, **DHCP**, assumes that a properly
configured DHCP server is available to provide TCP/IP settings to Network
Management Cards. You can also configure the setting for BOOTP.
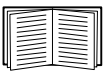
> A user configuration (.ini) file can function as a BOOTP or DHCP
> boot file. For more information, see the TCP/IP configuration
> section of the Network Management Card *User's Guide*, available
> from the *Utility* CD or the APC Web site, **www.apc.com**.
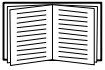
If neither of these servers is available, see one of these sections to configure the needed TCP/IP settings:

- "Device IP Configuration Wizard" on page 5
- "Local access to the command line interface" on page 8
- "Remote access to the command line interface" on page 8
- "User interface display" on page 10.

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

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

When the Network Management Card reboots, the BOOTP server provides it with the TCP/IP settings.

- If you specified a bootup file name, the Network Management Card attempts to transfer that file from the BOOTP server using TFTP or FTP. The Network Management Card assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Network Management Card remotely through its Web interface or command line interface; the user name and password are both **apc**, by default.
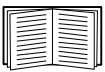
To create a bootup file, see your BOOTP server documentation.

DHCP. You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Network Management Card.
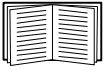
This section summarizes the Network Management Card's communication with a DHCP server. For more detail about how a DHCP server can configure the network settings for a Network Management Card, see "DHCP Configuration" in the Network Management Card *User's Guide* on the *Utility* CD.

1. The Network Management Card sends out a DHCP request that uses the following to identify itself:
   – A Vendor Class Identifier (APC by default)
   – A Client Identifier (by default, the MAC address of the Network Management Card)
   – A User Class Identifier (by default, the identification of the application firmware installed on the Network Management Card)

2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the Network Management Card needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Network Management Card can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The Card does not require this cookie by default).

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

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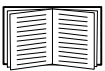
See your DHCP server documentation to add code to the Vendor Specific Information option.

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

Local access to the command line interface

You can use a computer connected to the serial port on the front of the Network Management Card to access the command line interface.

1. Select a serial port at the local computer, and disable any service that uses that port.

2. Use the provided serial cable (part number 940-0299) to connect the selected port to the serial port on the front panel of the Network Management Card.

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. Use **apc** for the user name and password.
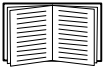
See "Command line interface" on page 9 to finish the configuration.

Remote access to the command line interface

From any computer on the same network as the Network Management Card, you can use ARP and Ping to assign an IP address to the Network Management Card, and then use Telnet to access its command line interface and configure the other TCP/IP settings.

Note: After the Network Management Card has its IP address configured, you can use Telnet, without first using ARP and Ping, to access that Network Management Card.

1. Use the MAC address of the Network Management Card in the ARP command to define the IP address.

Note: Look for the MAC address on the bottom of the Network Management Card or on the Quality Assurance slip included in the package.

For example, to define 156.205.14.141 as the IP address of a Network Management Card with 00 c0 b7 63 9f 67 as its MAC address, use one of the following commands:
– Windows command format:

```
arp -s 156.205.14.141 00-c0-b7-63-9f-67
```
– LINUX command format:

```
arp -s 156.205.14.141 00:c0:b7:63:9f:67
```

2. Use Ping with a size of 113 bytes to assign the IP address defined by the ARP command. For the IP address defined in step 1, use one of the following commands:
   – Windows command format:

   ```
   ping 156.205.14.141 -l 113
   ```
   – LINUX command format:

   ```
   ping 156.205.14.141 -s 113
   ```

3. Use Telnet to access the Network Management Card at its newly assigned IP address. For example:

   ```
   telnet 156.205.14.141
   ```

4. Use **apc** for both user name and password.
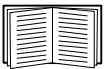
   See "Command line interface" on this page to finish the configuration.

Command line interface

After you log on at the command line interface, as described in "Local access to the command line interface" on page 8 or "Remote access to the command line interface" on page 8, you can manually configure network settings.

1. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Network Management Card.

2. Use these three commands to configure network settings. (Text in italics indicates a variable.)

   a. tcpip -i *yourIPaddress*

   b. tcpip -s *yourSubnetMask*

   c. tcpip -g *yourDefaultGateway*

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

   For example, to set a system IP address of 156.205.14.141, type the following command and press ENTER:
   ```
   tcpip -i 156.205.14.141
   ```

3. Type reboot. The Network Management Card restarts to apply the changes.

User interface display

To configure the IP address of a Network Management Card at the user interface display of the UPS:

1. If you plan to manually assign the network settings, contact your system administrator to obtain a valid IP address, subnet mask, and default gateway for the Network Management Card.

2. At the user interface display, press the **UPS System** icon.

3. Select **Configuration**, then **User Configuration**.

4. At the prompt, enter the **user** password for your UPS (**apc**, by default), then select **NMC Settings**.

5. For the Network Management Card you are configuring, select **Configure NMC Settings.**

6. In the **Network settings mode** drop-down list, select the network configuration option for your system: **Manual**, **BootP**, **DHCP**, or **DHCP & BootP**.
   – If you select **Manual**, enter the IP address, subnet mask, and default gateway you obtained in step 1.
   – If you select **BootP**, **DHCP**, or **DHCP & BootP**, a DHCP or BOOTP server will assign the IP address, subnet mask, and default gateway for the Network Management Card.

7. Press **Apply** to save your changes.

How to Recover from a Lost Password

You can use a local computer that connects to the Management Card through the serial port to access the command line interface.

1. Select a serial port at the local computer, and disable any service that uses that port.

2. Connect the provided serial cable (part number 940-0299) to the selected port at the computer and to the configuration port at the Management Card.

3. Run a terminal program (such as HyperTerminal®) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   – The serial port is not in use by another application.
   – The terminal settings are correct as specified in step 3.
   – The correct cable is being used as specified in step 2.

5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.

6. Press ENTER, repeatedly if necessary, to display the **User Name** prompt again, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)

7. At the command line interface, use the following commands to change the **User Name** and **Password** settings, both of which are now **apc**:

   ```
   user -an yourAdministratorName

   user -ap yourAdministratorPassword
   ```

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

   ```
   user -an Admin
   ```

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

How to Access a Configured Network Management Card

Overview

After the Network Management Card is running on your network, you can use the interfaces summarized here: Web interface, Telnet and SSH, SNMP, FTP, and SCP.
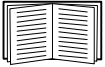
For more information about the interfaces, see the *User's Guide*.
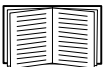
Web interface

Use Microsoft Internet Explorer® (IE) 7.x or higher (on Windows operating systems only) or Mozilla® Firefox® 3.0.6 or higher (on all operating systems) to access the Web interface of the Network Management Card. Other commonly available browsers may work but have not been fully tested by APC.

You can use either of the following protocols when you use the Web interface:

- The HTTP protocol (enabled by default), which provides authentication by user name and password but no encryption.
- The HTTPS protocol, which provides extra security through Secure Socket Layer (SSL); encrypts user names, passwords, and data being transmitted; and authenticates Network Management Cards by means of digital certificates.

To access the Web interface and configure the security of your device on the network:

1. Address the Network Management Card by its IP address (or its DNS name, if a DNS name is configured).

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator).

3. To enable or disable the HTTP or HTTPS protocol, use the **Network** menu on the **Administration** tab, and select the **access** option under the **Web** heading on the left navigation menu.

See the *Security Handbook*, available on the Network Management Card *Utility* CD or from the APC Web site, **www.apc.com**, for more information on selecting and configuring network security.

Telnet and SSH

You can access the command line interface through Telnet or Secure SHell (SSH), depending on which is enabled. To enable these access methods, select the **Administration** tab, the **Network** menu on the top menu bar, and the **access** option under **Console** on the left navigation 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 command line interface of the Network Management Card from any computer on the same subnet:

1. At a command prompt, use the following command line, and press ENTER:

   ```
   telnet address
   ```

   As *address*, use the Network Management Card's IP address (or DNS name, if configured).

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

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 command line interface. SSH encrypts user names, passwords, and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.
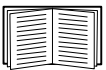
See the *User's Guide* for more information on configuring and using SSH.

Simple Network Management Protocol (SNMP)

SNMPv1 only. After you add the PowerNet® MIB to a standard SNMP MIB browser, you can use that browser to access the Network Management Card. All user names, passwords, and community names for SNMP are transferred over the network as plain text. The default read community name is **public**; the default read/write community name is **private**.

SNMPv3 only. For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps. The default settings are **no authentication** and **no privacy**.

Note: To use SNMPv3, you must have a MIB program that supports SNMPv3.

The Network Management Card supports SHA or MD5 authentication and AES or DES encryption.

SNMPv1 and SNMPv3. To use InfraStruXure Central to manage the Network Management Card on the public network of an InfraStruXure system, you must have SNMPv1 enabled in the unit interface. Read access allows InfraStruXure Central to receive traps from the Network Management Card. Write access is required while you set InfraStruXure Central as a trap receiver.

To enable or disable SNMP access, you must be an Administrator. Select the **Administration** tab, select the **Network** menu on the top menu bar, and use the **access** option under **SNMPv1** or **SNMPv3** on the left navigation menu.

FTP and SCP

You can use FTP (enabled by default) or SCP to transfer downloaded firmware to the Network Management Card, or to access a copy of the Network Management Card's event or data logs.

To use InfraStruXure Central to manage the UPS, you must have the **FTP Server** option enabled in the Network Management Card interface.

To enable or disable FTP server access, you must be an Administrator. Select the **Administration** tab, select the **Network** menu on the top menu bar, and use the **FTP Server** option on the left navigation menu.
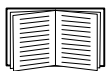
To transfer firmware, see the "File Transfers" chapter of the *User's Guide*.

To retrieve a copy of the event or data log, see the procedure "How to use FTP or SCP to retrieve log files" in the "Logs" chapter of the *User's Guide*.

Manage the security of your system
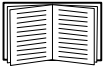
For detailed information on enhancing the security of your system after installation and initial configuration, see the *Security Handbook*, available on the Network Management Card *Utility* CD and on the APC Web site, **www.apc.com**.

Specifications

Physical

Size (H x W x D)	38.1 x 120.7 x 108 mm (1.50 x 4.75 x 4.25 in)
Weight	0.14 kg (0.30 lb)
Shipping weight	0.91 kg (2.01 lb)

Environmental

Elevation (above MSL)	
Operating	0 to 3000 m (0 to 10,000 ft)
Storage	0 to 15 000 m (0 to 50,000 ft)
Temperature	
Operating	-5 to 45°C (23 to 113°F)
Storage	-15 to 65°C (5 to 149°F)
Operating humidity	0 to 95%, non-condensing

Regulatory compliance

Radiated emissions	FCC Class A, VCCI Class A, ICES-003 Class A, EN 55022 Class A, AS/NZS CISPR 22, GOST-R 51318.22
Radiated immunity	GOST-R 51318.24, EN 55024

Radio Frequency Interference

⚠️ **Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.**

USA—FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. The user will bear sole responsibility for correcting such interference.

Canada—ICES

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan—VCCI

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講ずるように要求されることがあります。

Taiwan—BSMI

警告使用者：
這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻
干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

Australia and New Zealand

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. APC cannot accept responsibility for any failure to satisfy the protection requirements resulting from an unapproved modification of the product.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide a reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Korean 한국

A 급 기기 (업무용 방송통신기기)

이 기기는 업무용 (A 급) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정외의지역에서 사용하 는 것을 목적으로 합니다 .

APC Worldwide Customer Support

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

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
    - **www.apc.com** (Corporate Headquarters)
      Connect to localized APC Web sites for specific countries, each of which provides customer support information.
    - **www.apc.com/support/**
      Global support searching APC Knowledge Base and using e-support.
- Contact the APC Customer Support Center by telephone or e-mail.
    - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

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