Installation Manual

UPS Network Management Card 4

AP9644

990-91053A-001

Publication Date: October 2020

Schneider Electric

Schneider Electric IT Corporation Legal Disclaimer

The information presented in this manual is not warranted by the Schneider Electric IT Corporation to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric IT Corporation assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric IT Corporation. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC IT CORPORATION, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC IT CORPORATION OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC IT CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC IT CORPORATION RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Contents

Important Safety Information

Read the instructions carefully to become familiar with the equipment before trying to install, operate, service, or maintain it. The following special messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

NOTICE

NOTICE addresses practices not related to physical injury including certain environmental hazards, potential damage or loss of data.

Safety Information for the Network Management Card 4

The Network Management Card (NMC) contains a removable battery. If this battery is ingested, seek immediate medical attention.

⚠WARNING

HAZARD OF INTERNAL BURNS

- Do not ingest the battery.
- Keep batteries out of reach of children.

Failure to follow these instructions can result in serious injury or death.

NOTE: Secure the NMC to the UPS device's SmartSlot using screws to keep the battery out of reach.

Preliminary Information

Features

The Schneider Electric UPS Network Management Card (AP9644) discussed in this document is a Web-based product. Devices with the NMC installed can be managed using multiple open standards such as:

Hypertext Transfer Protocol (HTTP)	Secure SHell (SSH)
Simple Network Management Protocol versions 1, 2c and 3	Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
File Transfer Protocol (FTP)	Secure File Transfer Protocol (SFTP)
Syslog	Modbus

NOTE: Only HTTPS and SSH are enabled by default.

The **AP9644** Network Management Card:

- *Provides event logs.*
- *Enables you to set up notifications through event logging, e-mail, Syslog and SNMP traps.*
- *Provides support for PowerChute® Network Shutdown.*
- *Supports using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap Protocol (BOOTP) server to provide the network (TCP/IP) values of the NMC.*
- *Provides a selection of security protocols for authentication and encryption.*
- *Communicates with EcoStruxure IT and StruxureWare Data Center Expert.*
- *Supports Modbus TCP/IP, and Modbus RTU. For information on how to configure Modbus RTU, refer to the Modbus Documentation Addendum.*
- *Supports one universal input/output port, to which you can connect a temperature (AP9335T) or temperature/humidity sensor (AP9335TH).*

Supported Devices

The Network Management Card 4 is compatible with 3-phase Galaxy VS UPS devices.

Related documents

The following documentation is available on the Schneider Electric website:

- *UPS Network Management Card 4 Command Line Interface Guide*
- *UPS Network Management Card 4 Modbus Documentation Addendum*
- *Galaxy VS Modbus Register Map*
- *Security Handbook*
- *PowerNet® Management Information Base (MIB) Reference Guide*
- *Declaration of Conformity*

Inventory

The Network Management Card package includes the following items:

- *This Installation Manual*
- *UPS Network Management Card 4*
- *Micro-USB configuration cable (part number 960-0603)*
- *Temperature sensor (AP9335T)*
- *UPS Network Management Card 4 Modbus Documentation Addendum*
- *Network Management Card quality assurance test slip*
- *Warranty registration form*

Disclaimer

Schneider Electric is not responsible for damage sustained during reshipment of this product.

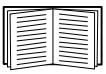
The Network Management Card 4 (NMC 4) is sensitive to static electricity. When handling the NMC, touch only the end plate while using one or more of these electrostatic-discharge devices (ESDs): wrist straps, heel straps, toe straps, or conductive shoes.

Please recycle

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

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

Changing Web UI Language



You can change the language the NMC Web interface is displayed in via the Web UI log in screen.

Installation in a UPS

How to install the card for different UPS models

To view the full list of compatible UPS in which an NMC can be installed, see Knowledge Base article FA237786 on the Schneider Electric website.

Step 1: Install the Network Management Card

You do not need to turn off power to install the NMC in a supported Galaxy UPS. If you want to turn off your UPS before installing the Network Management Card, see Knowledge Base article FA156132 on the Schneider Electric website.

The NMC is sensitive to static electricity. When handling the NMC, 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.

The Network Management Card (NMC) contains a removable battery. If this battery is ingested, seek immediate medical attention.

WARNING

HAZARD OF INTERNAL BURNS

- Do not ingest the battery.
- Keep batteries out of reach of children.

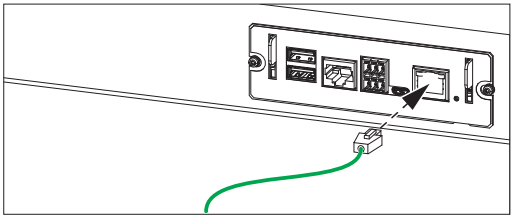
Failure to follow these instructions can result in serious injury or death.

NOTE: Secure the NMC to the UPS device's SmartSlot using screws to keep the battery out of reach.

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 NMC in the UPS card slot.

3. Connect a network interface cable to the 10/100/1000Base-T network connector 1 on the NMC.



When the network interface cable is connected, the NMC will attempt to obtain an IP address via DHCP. See “TCP/IP configuration methods” on page 11. **NOTE:** The card’s IP address will be displayed on the LCD of the UPS.

Step 2: Configure the Network Management Card

See “Quick Configuration” on page 7.

Quick Configuration

Overview

DHCP is enabled by default on the NMC. However, for a manual configuration, the following TCP/IP settings must be configured before the UPS Network Management Card (NMC) can operate on a network:

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

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.

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.

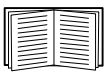
TCP/IP configuration methods

Use one of the following methods to define the TCP/IP settings needed by the Network Management Card for IPv4:

- “DHCP and BOOTP configuration” on page 7
- “How to Reset after a Forgotten Password” on page 12
- Networked computer:
  - “Remote access to the command line interface” on page 9

DHCP and BOOTP configuration

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

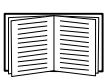


If neither of these servers is available, see “Remote access to the command line interface” on page 9 or “UPS User Interface Display” on page 11 to configure the needed TCP/IP settings.

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.

DHCP. You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Network Management Card (NMC).



This section summarizes the NMC's communication with a DHCP server.

1.The NMC sends out a DHCP request that uses the following to identify itself:

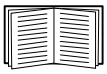
- A Vendor Class Identifier (APC by default)
- A Client Identifier (by default, the MAC address of the NMC)
- A User Class Identifier (by default, the identification of the application firmware installed on the NMC)

2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the NMC needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The NMC 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.

The NMC Web interface has options to utilize vendor-specific data to require the DHCP server to provide an "APC" cookie which will supply information to the NMC.

Local access to the web interface

For local access, use a computer that connects to the Network Management Card through the console port to access the command line interface:

1. Connect the provided micro-USB cable (part number 960-0603) from the USB port on the computer to the console port at the NMC.
2. In a supported browser, type “https://169.254.252.1” into the address bar, and press ENTER. **NOTE:** In firmware version 6.3 and below, the IP address used was “172.16.2.1”.
3. Use **apc** for both user name and password.

   NOTE: The user name will be “apc” at first log for the Super User account. You will be prompted to enter a new password after you log in.

If the micro-USB cable is connected to the computer while the NMC is booting up, the NMC will appear as an unrecognized device. To resolve the issue, unplug the micro-USB cable, and reconnect the cable when the NMC is fully booted.

NOTE: The NMC’s Status LED is solid green when it has completed its boot up process. Fore more information on the NMC’s LEDs, see Knowledge Base article FA265129.

Remote access to the command line interface

From any computer on the same network as the Network Management Card, you can obtain the IP address from the UPS HMI, and then use Secure Shell (SSH) to access its command line interface and configure the other TCP/IP settings.

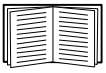
After the Network Management Card has its IP address configured, you can use SSH, to access that Network Management Card.

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

   ```
   ssh apc@156.205.14.141
   ```

   NOTE: This SSH command is for OpenSSH. The command may differ depending on the SSH tool used.
2. Use **apc** for both user name and password.

   NOTE: The user name will be “apc” at first log for the Super User account. You will be prompted to enter a new password after you log in.



See “Command line interface” on page 10 to finish the configuration.

Local access to the command line interface

For local access, use a computer that connects to the Network Management Card through the console port to access the command line interface:

1. Connect the provided micro-USB cable (part number 960-0603) from the USB port on the computer to the console port at the NMC.
2. Run a terminal program (e.g. 3rd party terminal emulator programs like HyperTerminal, PuTTY, or Tera Term) and configure the following:
   - **IP address:** 169.254.252.1. **NOTE: I**n firmware version 6.3 and below, the IP address used was “172.16.2.1”.
   - **Port:** 22
   - **Connection type:** SSH/SFTP
3. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
4. Use **apc** for both user name and password.

   NOTE: The user name will be “apc” at first log for the Super User account. You will be prompted to enter a new password after you log in.

If the micro-USB cable is connected to the computer while the NMC is booting up, the NMC will appear as an unrecognized device. To resolve the issue, unplug the micro-USB cable, and reconnect the cable when the NMC is fully booted.

NOTE: The NMC’s Status LED is solid green when it has completed its boot up process. Fore more information on the NMC’s LEDs, see Knowledge Base article FA265129.

Command line interface

After you log on at the command line interface, as described in “Remote access to the command line interface” on page 9, 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 this command to configure network settings. (Text in italics indicates a variable.)

   ```
   tcpip
   -i yourIPaddress
   -s yourSubnetMask
   -g yourDefaultGateway
   ```

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

   The command can be entered on one line. For example, to set a system IP address of 156.205.14.141, a Subnet Mask of 255.255.255.0 and a default

gateway of 156.205.14.1, type the following command and press ENTER:

```
tcpip -i 156.205.14.141 -s 255.255.255.0 -g 156.205.14.1
```

3. Use this command to get the NMC to use the static IP address, obtained in step 1, instead of getting its IP address from DHCP:

```
boot -b manual
```

UPS User Interface Display

The NMC IP address can be configured at the user interface 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 (Menu) icon, and then press the **Configuration** or **Control** icon to log in to the UPS.
3. At the prompt, enter the **user** password for your UPS (**admin**/**admin**, by default).
4. Select **Configuration > Network**. You can configure IPv4 or IPv6 settings for your NMC. Press the **Integrated NMC** button under your required IP format. **NOTE:** If you have an additional AP9644 card inserted in the NMC SmartSlot, you can configure its network settings by selecting **Optional NMC**.
5. Configure the Network Management Card network settings:
   a. **IPv4.** Select the network configuration option for your system: **Manual**, **DHCP**, or **BOOTP**.
      – If you select **Manual**, enter the IP address, subnet mask, and default gateway you obtained in step 1.
      – If you select **DHCP**, or **BOOTP**, a DHCP or BOOTP server will assign the IP address, subnet mask, and default gateway for the Network Management Card.
   b. **IPv6.** Select the network configuration option for your system: **Auto configuration**, or **Manual**.
      – If you select **Manual**, enter the IP address, and default gateway you obtained in step 1.
      – If you select **Auto configuration**, a DHCPv6 server will assign the IP address, and default gateway for the Network Management Card. You can select the DHCPv6 Mode: **Address and other information**, **non-address information only**, or **IPv6 never**.
6. Press **Ok** to save your changes.

How to Reset after a Forgotten Password

NOTE: Resetting your NMC will reset the card to its default configuration.

If you forget your password, you must use the **Reset** button on the NMC to wipe all configuration, including the password. Hold down the **Reset** button for 30 seconds, ensuring the Status LED is pulsing green during this time. When the Status LED changes to amber or orange, release the **Reset** button to allow the NMC to complete its reboot process.

After the NMC reboots, you must re-configure your NMC. See “Quick Configuration” on page 7.

How to Access a Configured Network Management Card

Overview

After the UPS Network Management Card (NMC) is running on your network, you can use the interfaces summarized here: Web interface, SSH, SNMP, FTP, and SFTP.

NOTE: Only HTTPS and SSH are enabled by default.

Web interface

The Network Management Card 4 Web interface is compatible with:

- Microsoft® Internet Explorer® (IE) 11 or higher, with compatibility view turned on.
- The latest releases of Mozilla® Firefox® or Google® Chrome®

Other commonly available browsers may work but have not been fully tested by Schneider Electric.

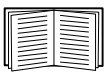
You can use either of the following protocols when you use the Web interface:

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

  NOTE: HTTP is disabled by default. The first log in to the Web UI must be using the HTTPS protocol.

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

1. Access 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 a Super User).
3. To enable or disable HTTPS, or enable HTTP, use the NMC Web interface.



See the *Network Management Card 4 Security Handbook*, available on the Schneider Electric website, for more information on selecting and configuring network security.

Command Line Interface access

You can access the command line interface through Secure SHell (SSH), which encrypts user names, passwords, and transmitted data. SSH is enabled by default.

To use SSH, you must first configure SSH and have an SSH client program installed on your computer.

To access the command line interface using SSH, at a command prompt enter:

```
ssh <username>@<IP address>
```

NOTE: This SSH command is for OpenSSH. The command may differ depending on the SSH tool used.

Simple Network Management Protocol (SNMP)

SNMPv1, SNMPv2c, and SNMPv3 are all disabled by default. You must configure community names in the Web UI before you can enable any version of SNMP.

To enable or disable SNMP access, you must be an Administrator. Use the NMC Web interface or Command Line interface to set it up.

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.

Use of SNMPv2c is supported by the SNMPv1 options.

SNMPv3 only. For SNMP GETs, 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.

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 EcoStruxure IT or StruxureWare Data Center Expert to manage the Network Management Card on the public network of an StruxureWare system, you must have SNMPv1 or SNMPv3 enabled in the unit interface. Read access allows EcoStruxure IT and StruxureWare Data Center Expert to receive alarms, data, and traps from the Network Management Card. Write access is required when you set EcoStruxure IT or StruxureWare Data Center Expert as an alarms, data, and trap receiver.

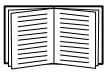
While both SNMPv1 and SNMPv3 are supported, it is recommended you use SNMPv3 as it is more secure and provides encryption and authentication.

SFTP

NOTE: By default, only SFTP is enabled. You can use SFTP once you have used SSH or HTTPS to create a user password.

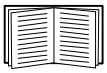
To use StruxureWare Data Center Expert to manage the UPS, you must have the **FTP Server** option enabled in the Network Management Card interface.

To enable or disable SFTP server access, you must be an Administrator. Use the NMC Web interface or Command Line interface to set it up.



The SCP interface is enabled when SSH is enabled, as they are part of the same protocol suite.

Manage the security of your system



For detailed information on enhancing the security of your system after installation and initial configuration, see the *Network Management Card 4 Security Handbook*, available on the Schneider Electric website.

Specifications AP9644

Physical	
Size (H x W x D)	38.1 x 120.7 x 108.0 mm (1.50 x 4.75 x 4.25 in)
Weight	0.14 kg (0.30 lb)
Shipping weight	0.91 kg (2.00 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	0 to 45 °C (32 to 113°F)
Storage	-5 to 45°C (23 to 113°F)
Operating humidity	0 to 95%, non-condensing

Regulatory compliance	
Radiated emissions	FCC Part 15 Class A, VCCI Class A, ICES-003 Class A, EN 55032 Class A, AS/NZS CISPR 32, 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

この装置は、クラスA機器です。この装置を住宅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要求されることがあります。

VCCI-A

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. Schneider Electric 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.

Worldwide Customer Support

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

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

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

990-91053A-001 **10/2020**