Installationshandbuch

UPS Network Management Card 3

AP9640, AP9641

990-9996B–005

Erscheinungsdatum: Mai 2019

Schneider Electric

Rechtlicher Hinweis von Schneider Electric IT Corporation

Die Schneider Electric IT Corporation gewährleistet nicht, dass die in dieser Bedienungsanleitung enthaltenen Informationen verbindlich, fehlerfrei oder vollständig sind. Diese Veröffentlichung stellt keinen Ersatz für einen ausführlichen betrieblichen und standortspezifischen Entwicklungsplan dar. Daher übernimmt Schneider Electric IT Corporation keinerlei Haftung für Schäden, Gesetzesübertretungen, unsachgemäße Installationen, Systemausfälle oder sonstige Probleme, die aus der Verwendung dieser Publikation resultieren können.

Die in dieser Veröffentlichung enthaltenen Informationen werden ohne Gewähr bereitgestellt und wurden ausschließlich zu dem Zweck zusammengestellt, den Entwurf und Bau von Datenzentren zu bewerten. Diese Veröffentlichung wurde von Schneider Electric IT Corporation nach bestem Wissen und Gewissen erstellt. Wir übernehmen jedoch keine Haftung oder Gewährleistung – weder ausdrücklich noch stillschweigend – für die Vollständigkeit oder Richtigkeit der Informationen in dieser Veröffentlichung.

KEINESFALLS HAFTEN SCHNEIDER ELECTRIC IT CORPORATION, MUTTER-, SCHWESTER- ODER TOCHTERGESELLSCHAFTEN VON SCHNEIDER ELECTRIC IT CORPORATION ODER DEREN JEWEILIGE VERANTWORTLICHE, DIREKTOREN ODER MITARBEITER FÜR DIREKTE, INDIREKTE, IN DER FOLGE ENTSTANDENE, SCHADENERSATZFORDERUNGEN BEGRÜNDENDE, SPEZIELLE ODER BEILÄUFIG ENTSTANDENE SCHÄDEN (AUCH NICHT FÜR ENTGANGENE GESCHÄFTE, VERTRÄGE, EINKÜNFTE ODER VERLORENE DATEN BZW. INFORMATIONEN SOWIE UNTERBRECHUNGEN VON BETRIEBSABLÄUFEN, UM NUR EINIGE ZU NENNEN), DIE AUS ODER IN VERBINDUNG MIT DER VERWENDUNG ODER UNMÖGLICHKEIT DER VERWENDUNG DIESER PUBLIKATION ODER IHRER INHALTE RESULTIEREN ODER ENTSTEHEN KÖNNEN, UND ZWAR AUCH DANN NICHT, WENN SCHNEIDER ELECTRIC IT CORPORATION VON DER MÖGLICHKEIT SOLCHER SCHÄDEN AUSDRÜCKLICH UNTERRICHTET WURDE. SCHNEIDER ELECTRIC IT CORPORATION BEHÄLT SICH DAS RECHT VOR, HINSICHTLICH DER PUBLIKATION, IHRES INHALTS ODER FORMATS JEDERZEIT UNANGEKÜNDIGT ÄNDERUNGEN ODER AKTUALISIERUNGEN VORZUNEHMEN.

Das Urheberrecht, das Recht am geistigen Eigentum und alle anderen Eigentumsrechte an den vorliegenden Inhalten (auch in Form von Software, Ton- und Videoaufzeichnungen, Text und Fotografien, um nur einige zu nennen) verbleibt bei Schneider Electric IT Corporation oder seinen Lizenzgebern. Alle Rechte am Inhalt, die hierin nicht ausdrücklich eingeräumt werden, bleiben vorbehalten. Es werden keine Rechte jeglicher Art an Personen lizenziert, zugewiesen oder anderweitig übertragen, die Zugang zu diesen Informationen haben.

Diese Veröffentlichung darf nicht – weder vollständig noch teilweise – weiterverkauft werden.



This manual is available in English on the APC Web site (www.apc.com).

Dieses Handbuch ist in Deutsch auf der APC Webseite (www.apc.com) verfügbar.

Данное руководство на русском языке доступно на сайте APC (www.apc.com)

本マニュアルの日本語版は APC ウェブサイト（www.apc.com）からダウンロードできます。

在 APC 公司的网站上（www.apc.com）有本手册的中文版。

Inhaltsverzeichnis

Wichtige Sicherheitsinformationen 1

Sicherheitsinformationen für die Netzwerkmanagement-Karte 3 2

Einleitende Informationen 3

Funktionen 3

Unterstützte Geräte 4

Zugehörige Dokumente 4

Lieferumfang 4

Haftungsausschluss 5

Ändern der Sprache der Web-Benutzeroberfläche 5

Einbau in eine USV. 6

Einbau der Karte in unterschiedliche USV-Modelle 6

Schritt 1: Einbauen der Netzwerkmanagement-Karte 6

Schritt 2: Konfigurieren der Netzwerkmanagement-Karte . . 7

Einbau in einem Erweiterungsgehäuse oder Dreifach-Erweiterungsgehäuse. 8

Verwendung eines Erweiterungsgehäuses 8

Schritt 1: Trennen des Gehäuses von der Stromversorgung . .8

Schritt 2: Einbauen der Netzwerkmanagement-Karte 8

Schnellkonfiguration 10

Übersicht 10

Verfahren für die TCP/IP-Konfiguration 10

Konfigurationsdienstprogramm für IP-Adressen 11

Konfiguration über BOOTP und DHCP 11

Lokaler Zugriff auf die Befehlszeilenoberfläche 14

Remotezugriff auf die Befehlszeilenoberfläche 15

Befehlszeilenoberfläche 16

Dienstprogramm für INI-Dateien 16

USV-Benutzeroberfläche 17

Zurücksetzen bei vergessenem Passwort 18

Zugriff auf eine konfigurierte Netzwerkmanagement-Karte . . . 19

Übersicht 19

Weboberfläche 19

Zugriff auf die Befehlszeilenoberfläche – SSH und Telnet . 20

Simple Network Management Protocol (SNMP) 21

SCP und FTP 22

Sicherheitsverwaltung des Systems 22

Installation mehrerer Management-Karten 23

Übersicht 23

Vor der Installation 23

Zwei Modelle von Erweiterungsgehäusen 24

Installation von Karten in ein Erweiterungsgehäuse 24

Serielles Setup beim Einbau von Karten in ein Erweiterungsgehäuse 24

Technische Daten von AP9640, AP9641 25

Wichtige Sicherheitsinformationen

Lesen Sie die Anweisungen sorgfältig durch und machen Sie sich mit dem Gerät vertraut, bevor Sie versuchen, es zu installieren, zu bedienen, zu reparieren oder zu warten. In diesem Handbuch bzw. auf dem Gerät sind hin und wieder die folgenden speziellen Hinweise zu sehen, die Sie vor potenziellen Gefahren warnen oder Ihre Aufmerksamkeit auf Informationen richten sollen, die eine Vorgehensweise verdeutlichen oder vereinfachen.



Wenn zusätzlich zu einem Sicherheitskennzeichen mit einem Gefahren- oder Warnhinweis dieses Symbol zu sehen ist, wird auf eine elektrische Gefahr hingewiesen, die bei Nichtbeachtung der Anweisungen zu Verletzungen führen kann.



Dieses Symbol ist eine Sicherheitswarnung. Es weist auf mögliche Verletzungsgefahren hin. Beachten Sie alle Sicherheitshinweise, die auf dieses Symbol folgen, um mögliche schwere oder tödliche Verletzungen zu verhindern.

⚠ GEFAHR

Gefahr weist auf eine gefährliche Situation hin, die bei Nichtvermeidung zu Tod oder schweren Verletzungen **führen wird**.

⚠WARNUNG

WARNUNG zeigt eine potenziell gefährliche Situation an, die, wenn sie nicht verhindert wird, zu einer tödlichen oder schweren Verletzung **führen kann**.

⚠VORSICHT

VORSICHT zeigt eine potenziell gefährliche Situation an, die, wenn sie nicht verhindert wird, zu einer kleineren oder mittelschweren Verletzung **führen kann**.

HINWEIS

HINWEIS verweist auf Praktiken, die nicht zu einer Körperverletzung führen, einschließlich bestimmter Umweltgefahren, möglicher Schäden oder Datenverlust.

Sicherheitsinformationen für die Netzwerkmanagement-Karte 3

Die Netzwerkmanagement-Karte (NMC) enthält eine herausnehmbare Batterie. Wenn diese Batterie verschluckt wird, müssen Sie sich umgehend in ärztliche Behandlung begeben

⚠ WARNUNG

GEFAHR INTERNER VERBRENNUNGEN

- Die Batterie darf nicht verschluckt werden.
- Die Batterien müssen von Kinder ferngehalten werden.

Die Nichtbeachtung dieser Vorschrift kann zu schweren Verletzungen oder zum Tode führen.

Hinweis: Befestigen Sie die NMC mit Schrauben auf dem SmartSlot des USV-Geräts, sodass sich die Batterie außer Reichweite befindet.

Einleitende Informationen

Funktionen

Bei den im vorliegenden Dokument beschriebenen USV-Netzwerkmanagement-Karten (AP9640 und AP9641) von Schneider Electric handelt es sich um webbasierte, IPv6-fähige Produkte. Geräte mit installierter Netzwerkmanagement-Karte können mithilfe verschiedener offener Standards verwaltet werden.



Hypertext Transfer Protocol (HTTP)	Secure SHell (SSH)
Simple Network Management Protocol Version 1, 2c und 3	Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
File Transfer Protocol (FTP)	Secure Copy (SCP)
Telnet	Syslog
RADIUS	Modbus
BACnet	Extensible Authentication Protocol (EAP) over LAN (EAPoL)

Die **AP9640**-Netzwerkmanagement-Karte:

- *Bietet Funktionen zur Steuerung der USV und zur planmäßigen Durchführung von Selbsttests an der USV.*
- *Liefert Daten- und Ereignisprotokolle.*
- *Bietet die Möglichkeit, Benachrichtigungen mithilfe von Ereignisprotokollierung, E-Mail, Syslog und SNMP-Traps einzurichten.*
- *Bietet Unterstützung für PowerChute® Network Shutdown.*
- *Unterstützt die Verwendung eines DHCP-Servers (Dynamic Host Configuration Protocol) oder eines BOOTP-Servers (BOOTstrap Protocol) zur Bereitstellung der TCP-/IP-Netzwerkparameter der Netzwerkmanagement-Karte.*
- *Ermöglicht das Exportieren einer benutzerdefinierten Konfigurationsdatei (INI-Datei) von einer konfigurierten Karte an mindestens eine unkonfigurierte Karte, ohne dass die Datei dazu in eine Binärdatei konvertiert werden muss.*
- *Bietet mehrere Sicherheitsprotokolle für Authentifizierung und Verschlüsselung.*
- *Kommuniziert mit StruxureWare Data Center Expert oder StruxureWare Operations.*
- *Unterstützt Modbus TCP/IP.*

Die **AP9641**-Netzwerkmanagement-Karte verfügt über sämtliche Funktionen der AP9640-Netzwerkmanagement-Karte und bietet darüber hinaus folgende Funktionen:

- *Zwei USB-Anschlüsse, die das Aktualisieren der USV-Firmware über einen USB-Stick unterstützen.*
- *Unterstützung für zwei universelle Eingabe-/Ausgabe-Anschlüsse, die mit folgenden Geräten verbunden werden können:*
  - Temperatur- (AP9335T) oder Temperatur-/Feuchtigkeitssensoren (AP9335TH)
  - Eingabe-/Ausgabe-Relaisstecker mit Unterstützung für zwei Eingangskontakte und ein Ausgangsrelais (mithilfe des optionalen E/A-Zusatzmoduls AP9810 für potenzialfreie Kontakte)
- *Unterstützung von Modbus RTU über den universellen E/A-Port 2 zusätzlich zu Modbus TCP/IP. Informationen zur Konfiguration von Modbus RTU finden Sie im Modbus-Dokumentationsanhang.*

Unterstützte Geräte

Die Netzwerkmanagement-Karte 3 ist kompatibel mit allen derzeit lieferbaren Smart-UPS®-Geräten mit einem SmartSlot (SMT/SMX/SRT) und Online-Smart-USV (SURT) der vorherigen Generation.

Zugehörige Dokumente

Folgende Dokumentation ist auf der APC-Website abrufbar:

- *Benutzerhandbuch für die USV-Netzwerkmanagement-Karte 3*
- *Befehlszeilenhandbuch für die USV-Netzwerkmanagement-Karte 3*
- *Modbus-Dokumentationsanhang für die USV-Netzwerkmanagement-Karte 3 (nur AP9641)*
- *Modbus-Registerkarten für die USV-Netzwerkmanagement-Karte 3*
- *Dienstprogramme zum Upgraden der Netzwerkmanagement-Karte*
- *Sicherheitshandbuch*
- *PowerNet® Management Information Base (*MIB) *Referenzhandbuch*
- *Konformitätserklärung*

Lieferumfang

Die folgenden Teile sind im Lieferumfang der Netzwerkmanagement-Karte enthalten:

- *Dieses Installationshandbuch*
- *USV-Netzwerkmanagement-Karte 3*
- *Micro-USB-Konfigurationskabel (Teilenummer 960-0603)*
- *Temperatursensor (AP9335T) – nur Netzwerkmanagement-Karte AP9641*
- *Qualitätskontrollabschnitt der Netzwerkmanagement-Karte*
- *Garantie-Registrierungskarte*

Der Qualitätskontrollabschnitt enthält die MAC-Adresse. Sie benötigen diese Adresse eventuell, wenn Sie die in “Konfigurationsdienstprogramm für IP-Adressen“ auf Seite 11 beschriebenen Verfahren durchführen. Sie finden die MAC-Adresse auch auf der Unterseite Ihrer Netzwerkmanagement-Karte.

Haftungsausschluss

Schneider Electric haftet nicht für während der Rücksendung dieses Produkts aufgetretene Schäden.



Die Netzwerkmanagement-Karte 3 (NMC 3) reagiert empfindlich auf statische Elektrizität. Berühren Sie bei der Handhabung der Netzwerkmanagement-Karte nur die Endplatte und verwenden Sie eine oder mehrere dieser Elektrostatik-Schutzvorrichtungen (ESDs): Armbänder, Fersenbänder, Zehenschlaufen, leitfähige Schuhe.

Recycling



Die Verpackung besteht aus wiederverwertbarem Material. Bewahren Sie die Verpackung für die spätere Verwendung auf, oder entsorgen Sie sie ordnungsgemäß.



Management-Produkte enthalten auswechselbare Lithium-Knopfzellenbatterien – dies gilt auch für die Netzwerkmanagement-Karte. Halten Sie beim Entsorgen dieser Batterien die geltenden Vorschriften für das Recycling ein.

Ändern der Sprache der Web-Benutzeroberfläche

Sie können die Sprache, die in der Web-Benutzeroberfläche der Netzwerkmanagement-Karte angezeigt wird, über den Bildschirm für das Einloggen ändern. Weitere Informationen finden Sie im *Benutzerhandbuch* unter „Ändern der Sprache der Web-Benutzeroberfläche“.

Einbau in eine USV

Einbau der Karte in unterschiedliche USV-Modelle

Eine vollständige Auflistung kompatibler USVs, in denen eine Netzwerkmanagement-Karte eingebaut werden kann, finden Sie im Knowledge Base-Artikel FA237786 auf der APC-website.

Siehe “Installation mehrerer Management-Karten“ auf Seite 23.

Schritt 1: Einbauen der Netzwerkmanagement-Karte

Zum Einbauen der Netzwerkmanagement-Karte in eine USV der Modellreihen Smart-UPS oder Galaxy UPS muss die Stromversorgung nicht getrennt werden. Wenn Sie Ihre USV vor dem Einbau der Netzwerkmanagement-Karte abschalten möchten, rufen Sie die Knowledge Base auf der Support-Seite der Website www.apc.com auf und suchen Sie dort nach FA156132 (ID des entsprechenden Artikels).



Die Netzwerkmanagement-Karte reagiert empfindlich auf statische Elektrizität. Berühren Sie die Netzwerkmanagement-Karte nur an den Rändern und verwenden Sie dabei mindestens eine der folgenden Vorrichtungen zur elektrostatischen Entladung: antistatische Arm- bzw. Fußbänder oder leitendes Schuhwerk.

Die Netzwerkmanagement-Karte (NMC) enthält eine herausnehmbare Batterie. Wenn diese Batterie verschluckt wird, müssen Sie sich umgehend in ärztliche Behandlung begeben.

WARNUNG

GEFAHR INTERNER VERBRENNUNGEN

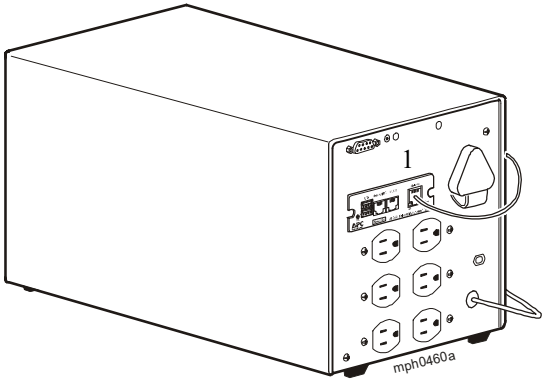
- Die Batterie darf nicht verschluckt werden.
- Die Batterien müssen von Kinder ferngehalten werden.

Die Nichtbeachtung dieser Vorschrift kann zu schweren Verletzungen oder zum Tode führen.

Hinweis: Befestigen Sie die NMC mit Schrauben auf dem SmartSlot des USV-Geräts, sodass sich die Batterie außer Reichweite befindet.

Weitere Informationen zur Position des USV-Kartensteckplatzes finden Sie in der Dokumentation zur USV.

1. Finden Sie den USV-Kartensteckplatz.
2. Verwenden Sie die Schrauben, mit denen das Abdeckblech befestigt ist, um die Netzwerkmanagement-Karte im Kartensteckplatz der USV zu befestigen.
3. Schließen Sie ein Netzwerkkabel an den 10/100/1000Base-T-Netzwerkanschluss 1 der Netzwerkmanagement-Karte an.



Sobald das Netzwerkkabel angeschlossen ist, versucht die Netzwerkmanagement-Karte, über DHCP eine IP-Adresse zu erhalten. Siehe “Verfahren für die TCP/IP-Konfiguration“ auf Seite 10.

Schritt 2: Konfigurieren der Netzwerkmanagement-Karte

Siehe „Schnellkonfiguration“ auf Seite 10.

Einbau in einem Erweiterungsgehäuse oder Dreifach-Erweiterungsgehäuse

Verwendung eines Erweiterungsgehäuses

Verwenden Sie ein Erweiterungsgehäuse oder ein Dreifach-Erweiterungsgehäuse, wenn in der USV kein Kartensteckplatz verfügbar ist.



Das einfache (AP9600) bzw. dreifache (AP9604) Erweiterungsgehäuse ist ausschließlich mit USV-Modellen kompatibel, die über einen seriellen DB9-Anschluss verfügen. Es ist nur mit folgenden USV-Modellen kompatibel: SURT, SURTA, SU, SUA und SUM.

Nach dem Einbau der USV-Netzwerkmanagement-Karte 3 (NMC 3) in das Gehäuse kommuniziert die Netzwerkmanagement-Karte mit der USV über die Kabelverbindung zwischen Gehäuse und USV.

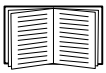
Schritt 1: Trennen des Gehäuses von der Stromversorgung

Stellen Sie sicher, dass das Erweiterungsgehäuse und das Dreifach-Erweiterungsgehäuse von der Stromversorgung getrennt wurden:

1. Trennen Sie das Gehäusekabel von der USV.
2. Falls das Gehäuse einen Wechselstromadapter (AP9505) verwendet, trennen Sie den Adapter vom Gehäuse.

Schritt 2: Einbauen der Netzwerkmanagement-Karte

Falls die USV mehrere Managementprodukte gleichzeitig verwendet, müssen Sie diese in der richtigen Reihenfolge installieren, damit sie einwandfrei funktionieren.



Siehe “Installation mehrerer Management-Karten“ auf Seite 23.



Die USV-Netzwerkmanagement-Karte reagiert empfindlich auf statische Elektrizität. Berühren Sie bei der Handhabung der Netzwerkmanagement-Karte nur die Endplatte und verwenden Sie eine oder mehrere dieser Elektrostatik-Schutzvorrichtungen (ESDs): Armbänder, Fersenbänder, Zehenschlaufen, leitfähige Schuhe.

Die Netzwerkmanagement-Karte (NMC) enthält eine herausnehmbare Batterie. Wenn diese Batterie verschluckt wird, müssen Sie sich umgehend in ärztliche Behandlung begeben.

⚠ WARNUNG

GEFAHR INTERNER VERBRENNUNGEN

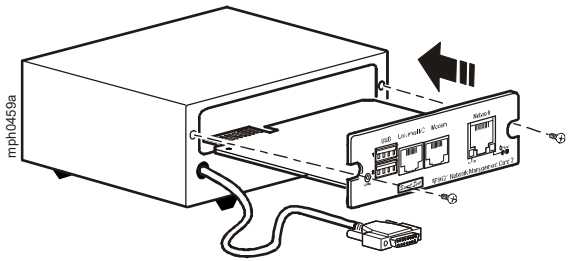
- Die Batterie darf nicht verschluckt werden.
- Die Batterien müssen von Kinder ferngehalten werden.

Die Nichtbeachtung dieser Vorschrift kann zu schweren Verletzungen oder zum Tode führen.

Hinweis: Befestigen Sie die NMC mit Schrauben auf dem SmartSlot des USV-Geräts, sodass sich die Batterie außer Reichweite befindet.

Falls ein Kabel an die serielle Schnittstelle der USV oder des Gehäuses angeschlossen ist, beenden Sie den APC-Dienst, der diese serielle Verbindung nutzt, und ziehen Sie das Kabel ab.

1. Wenn Sie ein Gehäuse installieren, verbinden Sie das Gehäuse mit dem seriellen Port der UPS.
2. Verwenden Sie die Schrauben, mit denen das Abdeckblech befestigt ist, um die Netzwerkmanagement-Karte im Erweiterungssteckplatz des Gehäuses zu befestigen.



3. Schließen Sie ein Netzwerkkabel an den 10/100/1000Base-T-Netzwerkanschluss an der Frontblende der Netzwerkmanagement-Karte an.
4. Bei Verwendung des Wechselstromadapters (AP9505) schließen Sie den Adapter an das Gehäuse an. Schließen Sie dann den Adapter an eine unabhängige Wechselstromversorgung an, damit die Netzwerkmanagement-Karte auch dann funktioniert, wenn die USV ausgeschaltet wird oder ausfällt.
5. Wenn Sie in Schritt 1 ein Kabel abgezogen haben, schließen Sie dieses Kabel erneut an der seriellen Schnittstelle des Gehäuses an und starten Sie den entsprechenden APC-Dienst erneut.
6. Siehe “Schnellkonfiguration“ auf Seite 10.

Schnellkonfiguration

Übersicht



Ignorieren Sie bitte die in diesem Kapitel beschriebenen Verfahren, wenn StruxureWare Data Center Expert in Ihr System integriert ist. Weitere Informationen finden Sie in der mit Ihrem StruxureWare-Gerät gelieferten Dokumentation.

Bevor die USV-Netzwerkmanagement-Karte im Netzwerk betrieben werden kann, müssen Sie die folgenden Einstellungen für TCP/IP festlegen:

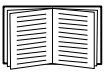
- IP-Adresse der Netzwerkmanagement-Karte
- Subnetzmaske
- Standardgateway



Wenn kein Standardgateway zur Verfügung steht, geben Sie die IP-Adresse eines Computers an, der sich in demselben Subnetz wie die Netzwerkmanagement-Karte befindet und normalerweise in Betrieb ist. Bei geringem Netzwerkverkehr verwendet die Netzwerkmanagement-Karte das Standardgateway, um das Netzwerk zu testen.



Verwenden Sie nicht die Loopback-Adresse (127.0.0.1) als Standardgateway-Adresse der Netzwerkmanagement-Karte. Damit deaktivieren Sie die Karte und müssen die TCP/IP-Einstellungen über eine lokale serielle Anmeldung auf die Standardwerte zurücksetzen.



Weitere Informationen über die Wächterfunktion des Standardgateways finden Sie im *Benutzerhandbuch* der Netzwerkmanagement-Karte im Abschnitt „Einführung“ unter „Wächterfunktionen“ auf der APC-Website.

Verfahren für die TCP/IP-Konfiguration

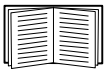
Verwenden Sie eine der folgenden Methoden, um die von der Netzwerkmanagement-Karte benötigten TCP/IP-Einstellungen für IPv4 zu konfigurieren:

- “Konfigurationsdienstprogramm für IP-Adressen“ auf Seite 11
- “Konfiguration über BOOTP und DHCP“ auf Seite 11
- “Zurücksetzen bei vergessenem Passwort“ auf Seite 18
- Ein mit dem Netzwerk verbundener Computer:
  - “Lokaler Zugriff auf die Befehlszeilenoberfläche“ auf Seite 14
  - “Remotezugriff auf die Befehlszeilenoberfläche“ auf Seite 15

Konfigurationsdienstprogramm für IP-Adressen

Das Konfigurationsdienstprogramm für IP-Adressen kann Netzwerkkarten ohne zugewiesene IP-Adresse erkennen. Sobald diese erkannt wurden, können Sie die IP-Adresseneinstellungen für die Karten konfigurieren.

Sie können außerdem nach bereits im Netzwerk vorhandenen Geräten suchen, indem Sie einen IP-Bereich für Ihre Suche eingeben. Das Dienstprogramm durchsucht die IP-Adressen in dem definierten Bereich und zeigt Netzwerkkarten an, die bereits über eine von DHCP zugewiesene IP-Adresse verfügen.



Detaillierte Informationen über das Dienstprogramm finden Sie in der Knowledge Base auf der Support-Seite der Website www.apc.com. Suchen Sie dort nach FA156064 (ID des entsprechenden Artikels). Informationen zur DHCP-Option 12 (AOS 5.1.5 oder höher) finden Sie im Knowledge Base-Artikel FA156110.

Systemanforderungen. Das Dienstprogramm kann auf den Betriebssystemen Microsoft Windows 2000, Windows Server® 2003, Windows Server 2008, Windows Server 2012 und auf der 32-Bit- und 64-Bit-Version von Windows XP, Windows Vista, Windows 2008, Windows 7, Windows 8 und Windows 10 ausgeführt werden.

Dieses Dienstprogramm unterstützt Karten mit der Firmwareversion 3.0.x oder höher und wurde nur für IPv4 konzipiert.

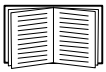
Installation. So installieren Sie das Dienstprogramm von einer heruntergeladenen EXE-Datei:

1. Gehen Sie auf www.apc.com/tools/download.
2. Filtern Sie nach Software Upgrades - Wizards and Configurators.
3. Wählen Sie das Dienstprogramm Network Management Device IP Configuration aus und laden Sie es herunter.
4. Öffnen Sie den Ordner, in den Sie das Dienstprogramm heruntergeladen haben, und starten Sie die EXE-Datei.

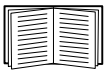
Nach der Installation ist das Dienstprogramm über die „Startmenü“-Option von Windows verfügbar.

Konfiguration über BOOTP und DHCP

Die Standardeinstellung für die TCP/IP-Konfiguration, **DHCP**, setzt voraus, dass ein ordnungsgemäß konfigurierter DHCP-Server verfügbar ist, von dem Netzwerkmanagement-Karten ihre TCP/IP-Einstellungen beziehen können. Sie können die Einstellung auch für BOOTP konfigurieren.



Eine benutzerdefinierte Initialisierungsdatei (.ini) kann als BOOTP- oder DHCP-Boot-Datei verwendet werden. Informationen hierzu finden Sie im *Benutzerhandbuch* zur Netzwerkmanagement-Karte unter „TCP/IP-Konfiguration“. Das Benutzerhandbuch kann auf der APC-Website, www.apc.com, abgerufen werden.



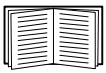
Falls kein solcher Server vorhanden ist, können Sie die erforderlichen TCP/IP-Einstellungen wie unter “Konfigurationsdienstprogramm für IP-Adressen“ auf Seite 11, “Lokaler Zugriff auf die Befehlszeilenoberfläche“ auf Seite 14, “Remotezugriff auf die Befehlszeilenoberfläche“ auf Seite 15 oder “USV-Benutzeroberfläche“ auf Seite 17 beschrieben konfigurieren.

BOOTP. Damit die Netzwerkmanagement-Karte einen BOOTP-Server zum Konfigurieren ihrer TCP/IP-Einstellungen verwenden kann, muss sie einen ordnungsgemäß konfigurierten, RFC951-konformen BOOTP-Server vorfinden.

Geben Sie in der Datei BOOTPTAB des BOOTP-Servers die MAC-Adresse, die IP-Adresse, die Subnetzmaske und das Standardgateway der Netzwerkmanagement-Karte sowie gegebenenfalls den Namen einer verwendeten Bootdatei ein. Die MAC-Adresse befindet sich auf der Unterseite der Netzwerkmanagement-Karte oder auf dem Qualitätskontrollabschnitt im Karton.

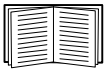
Beim Neustart der Netzwerkmanagement-Karte werden die TCP/IP-Einstellungen vom BOOTP-Server bereitgestellt.

- Wenn Sie den Namen einer Bootdatei eingegeben haben, versucht die Netzwerkmanagement-Karte, die betreffende Datei über TFTP oder FTP vom BOOTP-Server zu laden. Die Netzwerkmanagement-Karte übernimmt alle Einstellungen aus der Bootdatei.
- Wenn Sie keine Bootdatei angeben, können Sie die anderen Einstellungen der Netzwerkmanagement-Karte per Remotezugriff über die Weboberfläche oder über die Befehlszeilenoberfläche der Karte konfigurieren; Benutzername und Kennwort lauten in der Grundeinstellung **apc**.



Informationen zur Erstellung einer Initialisierungsdatei finden Sie in der Dokumentation Ihres BOOTP-Servers.

DHCP. Die TCP/IP-Einstellungen für die Netzwerkmanagement-Karte (NMC) können mit einem RFC2131/RFC2132-konformen DHCP-Server konfiguriert werden.



Dieser Abschnitt beschreibt die Kommunikation der Netzwerkmanagement-Karte mit einem DHCP-Server. Weitere Informationen dazu, wie die Netzwerkeinstellungen einer Netzwerkmanagement-Karte über einen DHCP-Server konfiguriert werden können, finden Sie im NMC-*Benutzerhandbuch* auf der APC-Website.

1. Die NMC sendet eine DHCP-Anfrage und identifiziert sich darin mit folgenden Angaben:
   - Einen Vendor Class Identifier (Herstellerklassenkennung, Standardwert: APC)
   - Einem Client Identifier (in der Grundeinstellung die MAC-Adresse der NMC)
   - Einem User Class Identifier (in der Grundeinstellung die Kennung der auf der NMC installierten Anwendungsfirmware).
2. Ein ordnungsgemäß konfigurierter DHCP-Server antwortet mit einem DHCP-Angebot, das alle Einstellungen enthält, die von der NMC für die Kommunikation im Netzwerk benötigt werden. Das DHCP-Angebot enthält auch die Option „Herstellerspezifische Informationen“ (DHCP-Option 43). Die NMC kann so konfiguriert werden, dass sie DHCP-Angebote ignoriert werden, die in der DHCP-Option 43 nicht das entsprechende APC-Cookie im nachfolgend aufgeführten Hexadezimalformat enthalten. (Die Karte benötigt dieses Cookie in der Grundeinstellung nicht.)

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

   Hierbei ist
   - das erste Byte (`01`) der Code
   - das zweite Byte (`04`) die Länge und
   - die übrigen Bytes (`31 41 50 43`) sind das APC-Cookie.



Die Dokumentation zum DHCP-Server enthält Informationen über das Hinzufügen von Code zur Option „HerstellerspezifischeInformationen“.

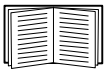


Die Web-Benutzeroberfläche der NMC verfügt über Optionen zur Nutzung von anbieterspezifischen Daten, um Daten von einem DHCP-Server anzufordern und ein „APC“-Cookie anzulegen, über welches Informationen an die Karte übermittelt werden. Weitere Informationen finden Sie im *Benutzerhandbuch*.

Lokaler Zugriff auf die Befehlszeilenoberfläche

Sie können über einen lokalen Computer, der über die serielle Schnittstelle der Netzwerkmanagement-Karte mit dieser verbunden ist, auf die Befehlszeile zugreifen:

1. Wählen Sie eine serielle Schnittstelle auf dem Computer aus und deaktivieren Sie sämtliche Dienste, die diese Schnittstelle verwenden.
2. Verbinden Sie das mitgelieferte Micro-USB-Kabel (Teilenummer 960-0603) mit dem am Computer ausgewählten Port und dem Konfigurationsport der NMC.
3. Führen Sie ein Terminalprogramm (z. B. Terminal-Emulatorprogramme Dritter wie HyperTerminal, PuTTy oder Tera Term) aus und konfigurieren Sie die ausgewählte Schnittstelle mit 9600 Bit/s, 8 Datenbits, keinem Paritätsbit, 1 Stoppbit und ohne Datenflusskontrolle. Speichern Sie die Änderungen.
4. Drücken Sie ggf. mehrmals die EINGABETASTE, um die Eingabeaufforderung **User Name (Benutzername)** aufzurufen.
5. Verwenden Sie **apc** als Benutzernamen (User Name) und als Kennwort (Password).



Informationen über das Abschließen der Konfiguration finden Sie unter “Befehlszeilenoberfläche“ auf Seite 16.

Remotezugriff auf die Befehlszeilenoberfläche

Auf einem Computer in demselben Netzwerk wie die Netzwerkmanagement-Karte können Sie dieser über die Befehle „ARP“ und „Ping“ eine IP-Adresse zuweisen. Danach können Sie über Secure Shell (SSH) auf die Befehlszeilenoberfläche der Netzwerkmanagement-Karte zugreifen und die anderen TCP/IP-Einstellungen konfigurieren.



Nach dem Konfigurieren der IP-Adresse für die Netzwerkmanagement-Karte können Sie über SSH auf die Netzwerkmanagement-Karte zugreifen, ohne zuerst „ARP“ und „Ping“ zu verwenden.

1. Verwenden Sie die MAC-Adresse der Netzwerkmanagement-Karte im Befehl ARP, um die IP-Adresse zu definieren.

   HINWEIS: Die MAC-Adresse befindet sich auf der Unterseite der Netzwerkmanagement-Karte oder auf dem Qualitätskontrollabschnitt im Karton.

   Wenn Sie beispielsweise die IP-Adresse 156.205.14.141 als Standard-IP-Adresse Netzwerkmanagement-Karte mit der MAC-Adresse 00 c0 b7 63 9f 67 definieren möchten, verwenden Sie dazu einen der folgenden Befehle:

   – Befehlsformat für Windows:

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

   – Befehlsformat für LINUX:

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

2. Verwenden Sie Ping mit einer Größe von 113 Byte, um die durch den ARP-Befehl festgelegte IP-Adresse zuzuweisen. Verwenden Sie für die in Schritt 1 definierte IP-Adresse einen der folgenden Befehle:

   – Befehlsformat für Windows:

   ```
   ping 156.205.14.141 -l 113
   ```

   – Befehlsformat für LINUX:

   ```
   ping 156.205.14.141 -s 113
   ```

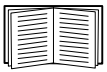
3. Verwenden Sie SSH, um unter der jetzt festgelegten IP-Adresse auf die Netzwerkmanagement-Karte zuzugreifen. Zum Beispiel:

   ```
   ssh -c 3des-cbc apc@156.205.14.141
   ```

   HINWEIS: Dieser SSH-Befehl gilt für OpenSSH. Der Befehl kann je nach verwendetem SSH-Tool abweichen.

4. Verwenden Sie **apc** als Benutzername (User Name) und als Kennwort (Password).

HINWEIS: Der Benutzername lautet beim ersten Einloggen über das Superuser-Konto „apc“. Nach dem Einloggen werden Sie aufgefordert, ein neues Passwort zu erstellen.



Informationen über das Abschließen der Konfiguration finden Sie unter “Befehlszeilenoberfläche“ auf Seite 16.

Befehlszeilenoberfläche

Nachdem Sie sich wie in “Lokaler Zugriff auf die Befehlszeilenoberfläche“ auf Seite 14 oder “Remotezugriff auf die Befehlszeilenoberfläche“ auf Seite 15 beschrieben an der Befehlszeilenoberfläche angemeldet haben, können Sie manuell die Netzwerkeinstellungen konfigurieren.

1. Wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Adresse, die Subnetzmaske und das Standardgateway für die Netzwerkmanagement-Karte zu erhalten.
2. Verwenden Sie zur Konfigurierung der Netzwerkeinstellungen diese drei Befehle. (Kursiver Text steht für eine Variable.)

   `tcpip`

   `-i` *`IhreIPAdresse`*

   `-s` *`IhreSubnetzMaske`*

   `-g` *`IhrStandardGateway`*

   Geben Sie für jede Variable einen numerischen Wert im Format *`xxx.xxx.xxx.xxx`* ein.

   Der Befehl kann in eine einzige Zeile eingegeben werden. Wenn Sie beispielsweise die System-IP-Adresse 156.205.14.141, die Subnetzmaske 255.255.255.0 und das Standardgateway 156.205.14.1 einstellen möchten, geben Sie den folgenden Befehl ein und drücken Sie anschließend die EINGABETASTE:

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

3. Geben Sie `reboot` ein. Die Netzwerkmanagement-Karte startet daraufhin neu, um die Änderungen zu übernehmen.

Dienstprogramm für INI-Dateien

Mit dem Dienstprogramm zum Exportieren von .ini-Dateien können Sie Einstellungen aus der .ini-Datei einer konfigurierten Netzwerkmanagement-Karte auf beliebig viele unkonfigurierte Netzwerkmanagement-Karten übertragen. Das Dienstprogramm und die Dokumentation können auf der APC-Website abgerufen werden und sind zudem im Knowledge Base-Artikel FA156117 auf www.apc.com/support enthalten.

USV-Benutzeroberfläche



Die Konfiguration der IP-Adresse der Netzwerkmanagement-Karte über die USV-Benutzeroberfläche ist nicht bei allen USV-Modellen möglich.

Bei USV-Anlagen der Modellreihe Smart-UPS mit Präfix SMT, SMX oder SRT kann die IP-Adresse der Netzwerkmanagement-Karte auf der Benutzeroberfläche der USV konfiguriert werden:

1. Wenn Sie die Netzwerkeinstellungen manuell zuweisen möchten, wenden Sie sich an Ihren Systemadministrator, um eine gültige IP-Adresse, die Subnetzmaske und das Standardgateway für die Netzwerkmanagement-Karte zu erhalten.
2. Betätigen Sie auf der Benutzeroberfläche das Symbol **Home**.
3. Wählen Sie **Configuration > Network** (Konfigurationsnetzwerk).
4. Geben Sie bei der entsprechenden Aufforderung das **Benutzerkennwort** für die USV ein (standardmäßig **apc**) und wählen Sie anschließend **NMC Settings** (NMC-Einstellungen).
5. Wählen Sie für die Netzwerkmanagement-Karte, die Sie konfigurieren, **Configure NMC Settings** (NMC-Einstellungen konfigurieren) aus.
6. Wählen Sie in der Dropdown-Liste Network settings mode (Netzwerk-Einstellungsmodus) die Netzwerk-Konfigurationsoptionen für Ihr System aus: **Manual** (Manuell), **BootP**, **DHCP** oder **DHCP & BootP**.
   - Wenn Sie **Manual** auswählen, geben Sie IP-Adresse, Subnetzmaske und Standardgateway ein, die Sie in Schritt 1 erhalten haben.
   - Wenn Sie **BootP**, **DHCP** oder **DHCP & BootP** auswählen, weist ein DHCP- oder BOOTP-Server automatisch IP-Adresse, Subnetzmaske und Standardgateway der Netzwerkmanagement-Karte zu.
7. Drücken Sie auf **Apply** (Anwenden), um die Änderungen zu speichern.

Zurücksetzen bei vergessenem Passwort



HINWEIS: Das Zurücksetzen Ihrer Netzwerkmanagement-Karte (NMC) setzt die Karte auf die Standardkonfiguration zurück..

Wenn Sie Ihr Passwort vergessen haben, müssen Sie die **Reset**-Taste auf der NMC verwenden, um die gesamte Konfiguration, einschließlich des Passworts, zu löschen. Halten Sie die **Reset**-Taste 20–25 Sekunden lang gedrückt und prüfen Sie, ob die Status-LED während dieser Zeit grün pulsiert. Wenn die Status-LED zu Gelb oder Orange wechselt, geben Sie die **Reset**-Taste frei, damit der Neustart der NMC abgeschlossen werden kann.

Nach dem Neustart der NMC müssen Sie die NMC neu konfigurieren. Siehe “Schnellkonfiguration“ auf Seite 10.



Es wird empfohlen, die .ini-Datei nach der Konfiguration Ihrer NMC zu exportieren, um Datenverluste im Falle eines vergessenen Passworts zu vermeiden. Weitere Informationen finden Sie im NMC-*Benutzerhandbuch* unter „Abrufen und Exportieren der .ini-Datei“.

Zugriff auf eine konfigurierte Netzwerkmanagement-Karte

Übersicht

Sobald die USV-Netzwerkmanagement-Karte im Netzwerk ausgeführt wird, können Sie die nachstehend beschriebenen Schnittstellen zum Zugriff auf die Karte verwenden: Web-Benutzeroberfläche, Telnet, SSH, SNMP, FTP sowie SCP.

Weitere Informationen zu den einzelnen Benutzeroberflächen finden Sie im *Benutzerhandbuch*.

Weboberfläche

Die Weboberfläche der Netzwerkmanagement-Karte 3 ist kompatibel mit:

- Windows® Betriebssystemen:
  - Microsoft® Internet Explorer® (IE) 11 oder höher mit aktivierter Kompatibilitätsansicht
  - Aktuelle Version von Microsoft® Edge®
- Allen Betriebssystemen:
  - Aktuelle Version von Mozilla® Firefox® oder Google® Chrome®

Eventuell funktionieren auch andere Browser, diese wurden jedoch von APC Schneider Electric nicht umfassend getestet.

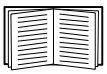
Sie können eines der folgenden Protokolle mit der Weboberfläche verwenden:

- Standardmäßig ist nur HTTPS aktiviert. Das HTTPS-Protokoll (standardmäßig aktiviert) bietet zusätzliche Sicherheit durch SSL (Secure Socket Layer), verschlüsselt Benutzernamen und Kennwörter sowie die übertragenen Daten und führt die Authentifizierung der Netzwerkmanagement-Karten über digitale Zertifikate durch.
- Das HTTP-Protokoll, bei dem die Authentifizierung über den Benutzernamen und das Passwort erfolgt, das aber keine Verschlüsselung bietet.

  HINWEIS: HTTP ist standardmäßig deaktiviert. Beim ersten Einloggen in der Web-Benutzeroberfläche muss das HTTPS-Protokoll verwendet werden.

So greifen Sie auf die Weboberfläche zu und konfigurieren die Sicherheit des Geräts im Netzwerk:

1. Greifen Sie über die IP-Adresse auf die Netzwerkmanagement-Karte zu (oder den DNS-Namen, sofern konfiguriert).
2. Geben Sie den Benutzernamen und das Kennwort ein (Grundeinstellung für Administratoren: **apc** und **apc**).
3. Verwenden Sie die Web-Benutzeroberfläche der NMC, um HTTPS zu deaktivieren oder HTTP zu aktivieren.



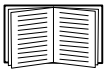
Weitere Informationen zur Auswahl und Konfiguration der Netzwerksicherheit finden Sie im *Sicherheitshandbuch*, das auf der APC-Website, www.apc.com, abgerufen werden kann.

Zugriff auf die Befehlszeilenoberfläche – SSH und Telnet

Der Zugriff auf die Befehlszeilenoberfläche erfolgt über Secure Shell (SSH) oder Telnet, abhängig davon, welche Option aktiviert ist. Verwenden Sie die Web-Benutzeroberfläche der Netzwerkmanagement-Karte, um diese Zugriffsmethoden zu aktivieren bzw. zu deaktivieren. Standardmäßig ist nur SSH aktiviert.

SSH für den Zugriff auf hoher Sicherheitsstufe. Wenn Sie für die Weboberfläche den hohen Sicherheitsstandard von SSL nutzen, verwenden Sie Secure SHell (SSH) für den Zugriff auf die Befehlszeilenoberfläche. SSH verschlüsselt Benutzernamen, Kennwörter und die übertragenen Daten.

Die Schnittstelle, die Benutzerkonten und die Zugriffsrechte des Benutzers sind immer gleich, unabhängig davon, ob der Zugriff auf die Befehlszeile über SSH oder Telnet erfolgt. Um SSH verwenden zu können, müssen Sie SSH jedoch zuerst konfigurieren und einen SSH-Client auf dem Computer installieren.



Weitere Informationen zur Konfiguration und Verwendung von SSH finden Sie im *Benutzerhandbuch*.

Wenn Sie über SSH auf die Befehlszeilenoberfläche zugreifen möchten, geben Sie in der Befehlszeile Folgendes ein:

```
ssh -c 3des-cbc <username>@<IP address>
```

HINWEIS: Dieser SSH-Befehl gilt für OpenSSH. Der Befehl kann je nach verwendetem SSH-Tool abweichen.

Telnet für den einfachen Zugriff. Telnet ist standardmäßig deaktiviert. Telnet bietet als einfachen Sicherheitsmechanismus eine Authentifizierung mit Benutzername und Kennwort. Es bietet jedoch nicht die Sicherheit einer verschlüsselten Anmeldung. Zum Zugriff über Telnet auf die Befehlszeilenoberfläche der Netzwerkmanagement-Karte von jedem Computer des selben Subnetzes aus, gehen Sie wie folgt vor:

1. Geben Sie an der Eingabeaufforderung die folgende Befehlszeile ein und betätigen Sie anschließend die EINGABETASTE:

   `telnet` *address*

   Verwenden Sie die IP-Adresse (oder den DNS-Namen, falls konfiguriert) der Netzwerkmanagement-Karte als Wert für *`address`*.

2. Geben Sie den Benutzernamen und das Kennwort ein (Standardwerte: **apc** und **apc** für einen Administrator, **device** und **apc** für einen Benutzer des Geräts).

Simple Network Management Protocol (SNMP)

SNMPv1, SNMPv2c und SNMPv3 sind standardmäßig deaktiviert. Sie müssen den Community-Namen in der Web-Benutzeroberfläche konfigurieren, bevor Sie eine beliebige Version von SNMP aktivieren können.

Der SNMP-Zugriff kann nur von einem Administrator aktiviert oder deaktiviert werden. Verwenden Sie zur Einrichtung die Web-Benutzeroberfläche oder die Befehlszeilenoberfläche der Netzwerkmanagement-Karte.

Nur SNMPv1. Nachdem Sie einem SNMP MIB-Browser die PowerNet®-MIB hinzugefügt haben, können Sie diesen Browser für den SNMP-Zugriff auf die Netzwerkmanagement-Karte verwenden. Alle Benutzernamen, Kennwörter und Community-Namen für SNMP werden als Klartext über das Netzwerk übertragen.

Die Verwendung von SNMPv2c wird durch die Optionen von SNMPv1 unterstützt.

Nur SNMPv3. Für die SNMP-Befehle GET und SET sowie für die Trap-Empfänger verwendet SNMPv3 ein System mit Benutzerprofilen zur Identifikation der Benutzer. Einem SNMPv3-Benutzer muss in der MIB-Software ein Benutzerprofil zugewiesen werden, damit er die SNMP-Befehle GET und SET ausführen, die MIB durchsuchen und Traps empfangen kann.

Zur Verwendung von SNMPv3 müssen Sie ein MIB-Programm einsetzen, das SNMPv3 unterstützt.

Die Netzwerkmanagement-Karte unterstützt SHA- oder MD5-Authentifizierung und AES oder DES-Verschlüsselung.

SNMPv1 und SNMPv3. Wenn Sie StruxureWare Data Center Expert zum Verwalten der Netzwerkmanagement-Karte im öffentlichen Netzwerk eines StruxureWare-Systems verwenden, müssen Sie auf der Benutzeroberfläche der Einheit SNMPv1 aktiviert haben. Der Lesezugriff erlaubt es dem StruxureWare Data Center Expert, Traps von der Netzwerkmanagement-Karte zu empfangen. Der Schreibzugriff ist erforderlich, um den StruxureWare Data Center Expert als Trap-Empfänger einzurichten.

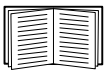
SCP und FTP

Sie können FCP oder SCP verwenden, um heruntergeladene Firmware auf eine Netzwerkmanagement-Karte zu übertragen, oder um auf eine Kopie der Ereignis- oder Datenprotokolle der Netzwerkmanagement-Karte zuzugreifen.

HINWEIS: Standardmäßig ist nur SCP aktiviert. Sie können SCP verwenden, sobald Sie über SSH oder HTTPS ein Benutzerpasswort erstellt haben.

Um StruxureWare Data Center Expert zum Verwalten der USV zu verwenden, müssen Sie in der Benutzeroberfläche der Netzwerkmanagement-Karte die Option **FTP-Server** aktiviert haben.

Die Option FTP-Server kann nur von einem Administrator aktiviert oder deaktiviert werden. Verwenden Sie zur Einrichtung die Web-Benutzeroberfläche oder die Befehlszeilenoberfläche der Netzwerkmanagement-Karte.

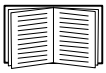


Informationen zur Übertragung von Firmware finden Sie im *Benutzerhandbuch*.

Die SCP-Oberfläche ist aktiviert, wenn SSH aktiviert ist, da sie zur selben Protokollsuite gehören. Weitere Informationen zur Konfiguration und Verwendung von SSH finden Sie im *Benutzerhandbuch*.

Informationen zum Abrufen einer Kopie der Ereignis- oder Datenprotokolle finden Sie im *Benutzerhandbuch*.

Sicherheitsverwaltung des Systems



Ausführliche Informationen zur Erhöhung der Systemsicherheit nach der Installation und Erstkonfiguration finden Sie im *Sicherheitshandbuch*, das auf der APC-Website, www.apc.com, abgerufen werden kann.

Installation mehrerer Management-Karten

Übersicht

Wenn Sie mehr als eine Netzwerkmanagement-Karte 3 installieren, müssen Sie die Karten in der in diesem Dokument beschriebenen Reihenfolge installieren. Die Karten müssen in der in diesem Dokument beschriebenen Reihenfolge eingebaut werden, da sie eine serielle Verbindung mit der USV teilen. Werden die Karten in einer anderen Reihenfolge eingebaut, kann dies dazu führen, dass sie nicht ordnungsgemäß funktionieren.

HINWEIS: Dieses Thema gilt nur für USV-Geräte auf dem USV-Link-Protokoll. Eine Aufschlüsselung der Geräte auf dem USV-Link-Protokoll erhalten Sie im Knowledge Base-Artikel FA230533.

Vor der Installation

In der nachstehenden Tabelle wird die Einbaureihenfolge der Management-Karten wiedergegeben. Management-Karten mit einer höheren Kontrolle über die USV haben eine höhere Priorität.

- Stufe 6: übt uneingeschränkte Kontrolle aus
- Stufe 5: übt starke, aber nicht uneingeschränkte Kontrolle aus
- Stufe 4: übt eingeschränkte Kontrolle aus
- Stufe 3: leitet Befehle an die USV weiter
- Stufe 2: übt keine Kontrolle aus
- Stufe 1: übt keine Kontrolle aus und muss am nächsten zur USV eingebaut werden

Management-Karte	**Priorität**
Netzwerkmanagement-Karte 3 (AP9640, AP9641)[1] Netzwerkmanagement-Karte 2 (AP9630, AP9631, AP9635)[2] Netzwerkmanagement-Karte 1 (AP9617, AP9618, AP9619)[2]	Stufe 6
Out-of-Band-Management-Karte (AP9608)[3]	Stufe 5
Relais-E/A-Modul (Relay I/O Module) (AP9613, AP9610)	Stufe 4
Interface Expander-Karte (Interface Expander Card) (AP9607[4], AP9624)	Stufe 3
Gebäudemanagement-Integrationskarte (Building Management Integration Card) (AP9622)[5]	Stufe 2
Umgebungsüberwachungskarte (Environmental Monitoring Card)	Stufe 1

1. Schließen Sie nicht mehr als zwei Netzwerkmanagement-Karten an eine USV an.
2. Die Netzwerkmanagement-Karten AP9617, AP9618, AP9619, AP9630, AP9631 und AP9635 werden eingestellt und durch AP9640 und AP9641 ersetzt.
3. AP9608 wird eingestellt und durch AP9635 ersetzt, die ebenfalls eingestellt wird.
4. AP9607 wird eingestellt und durch AP9624 ersetzt.
5. Pro USV immer nur eine Gebäudemanagement-Integrationskarte einbauen. AP9622 wird eingestellt und durch AP9635 ersetzt.

Zwei Modelle von Erweiterungsgehäusen

Wenn zusätzliche Steckplätze für Management-Karten zu denen in der USV benötigt werden, können ein oder mehrere Erweiterungsgehäuse bezogen werden.

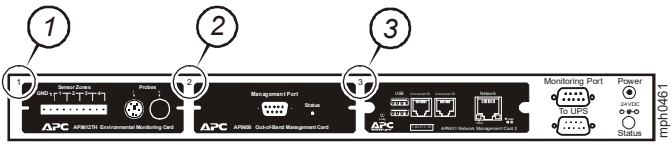
Gehäuse	Kompatible USVs
Erweiterungsgehäuse (AP9600), ein Steckplatz	USVs, die über einen DB9-Anschluss verfügen und nicht in Racks oder Gehäusen eingebaut sind.
Dreifach-Erweiterungsgehäuse (AP9604BLK), drei Steckplätze	USVs, die über einen DB9-Anschluss verfügen.

Das einfache (AP9600) bzw. dreifache (AP9604BLK) Erweiterungsgehäuse ist ausschließlich mit USV-Modellen kompatibel, die über einen seriellen DB9-Anschluss verfügen. Es ist nur mit folgenden USV-Modellen kompatibel: SURT, SURTA, SU, SUA und SUM.

Installation von Karten in ein Erweiterungsgehäuse

Installieren Sie die Karten mit der niedrigsten Priorität in einem beliebigen freien Kartensteckplatz in der USV. Verwenden Sie dann für die restlichen Karten mit höherer Priorität ein Erweiterungsgehäuse. Installation in ein Dreifach-Erweiterungsgehäuse:

- Installieren Sie jede Karte, beginnend mit der niedrigsten Prioritätsstufe (siehe “Vor der Installation“ auf Seite 23) in dem Steckplatz mit der niedrigsten Nummer.
- Wenn Sie eine Netzwerkmanagement-Karte installieren, bauen Sie diese in Steckplatz 3 ein, auch wenn ein anderer Steckplatz nicht belegt wird.



Serielles Setup beim Einbau von Karten in ein Erweiterungsgehäuse

Wenn Sie die Kapazität Ihrer Management-Karte durch das serielle Anschließen mehrerer Erweiterungsgehäuse (in abwärts verlaufender Konfiguration) erhöht haben, installieren Sie die Netzwerkmanagement-Karte im Steckplatz mit der höchsten Nummer.

Warnung: Schließen Sie nicht mehr als zwei Netzwerkmanagement-Karten oder eine Gebäudemanagement-Integrationskarte an eine USV an.

Wenn die Netzwerkmanagement-Karte in der USV werkseitig installiert ist, beachten Sie bitte stattdessen die Informationen unter “Wenn eine Netzwerkmanagement-Karte werkseitig installiert wurde.“ auf Seite 26.

Technische Daten von AP9640, AP9641

Abmessungen und Gewicht

Größe (H x B x T)	38,1 x 120,7 x 108,0 mm (1,50 x 4,75 x 4,25 in)
Gewicht	0,14 kg (0,30 lb)
Versandgewicht	0,91 kg (2,00 lb)

Anforderungen an die Umgebung

Höhe (über dem Meeresspiegel)	
Betrieb	0 bis 3.000 m (0 bis 10.000 ft)
Lagerung	0 bis 15.000 m (0 bis 50.000 ft)
Temperatur	
Betrieb	0 bis 45 °C (32 bis 113 °F)
Lagerung	-5 bis 45 °C (23 bis 113 °F)
Betriebsluftfeuchtigkeit	0 bis 95 %, nicht kondensierend

Einhaltung von gesetzlichen Vorschriften

Erfüllung der Normen zu Strahlungsemissionen	FCC Klasse A, VCCI Klasse A, ICES-003 Klasse A, EN 55022 Klasse A, AS/NZS CISPR 22, GOST-R 51318.22
Erfüllung der Normen zur Strahlungsimmunität	GOST-R 51318.24, EN 55024

cryptlib copyright Digital Data Security New Zealand Ltd 1998.

Copyright © 1990, 1993, 1994 Verwaltungsrat der Universität Kalifornien.
Alle Rechte vorbehalten.

Dieser Code wurde von Software abgeleitet, die Berkeley von Mike Olson zur Verfügung gestellt wurde.

Weiterverbreitung und Verwendung in nichtkompilierter oder kompilierter Form, mit oder ohne Veränderung, sind unter den folgenden Bedingungen zulässig:

1. Weiterverbreitete nichtkompilierte Exemplare müssen das obige Copyright, diese Liste der Bedingungen und den folgenden Haftungsausschluss im Quelltext enthalten.
2. Weiterverbreitete kompilierte Exemplare müssen das obige Copyright, diese Liste der Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder anderen Materialien, die mit dem Exemplar verbreitet werden, enthalten.
3. Sämtliche Werbematerialien, in denen Funktionen oder die Nutzung dieser Software erwähnt werden, müssen folgenden Vermerk enthalten:

   > Dieses Produkt enthält Software, die von der Universität Kalifornien, Berkeley und den Beitragsleistenden entwickelt wurde.

4. Weder der Name der Universität noch die Namen der Beitragsleistenden dürfen zum Kennzeichnen oder Bewerben von Produkten, die von dieser Software abgeleitet wurden, ohne spezielle vorherige schriftliche Genehmigung verwendet werden.

DIESE SOFTWARE WIRD VOM VERWALTUNGSRAT UND DEN BEITRAGSLEISTENDEN OHNE JEGLICHE SPEZIELLE ODER IMPLIZIERTE GARANTIEN ZUR VERFÜGUNG GESTELLT, DIE UNTER ANDEREM EINSCHLIESSEN: DIE IMPLIZIERTE GARANTIE DER MARKTGÄNGIGKEIT UND VERWENDBARKEIT DER SOFTWARE FÜR EINEN BESTIMMTEN ZWECK. AUF KEINEN FALL SIND DIE VERWALTUNGSRÄTE ODER DIE BEITRAGSLEISTENDEN FÜR IRGENDWELCHE DIREKTEN, INDIREKTEN, ZUFÄLLIGEN, SPEZIELLEN, BEISPIELHAFTEN ODER FOLGENDEN SCHÄDEN (UNTER ANDEREM VERSCHAFFEN VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN; EINSCHRÄNKUNG DER NUTZUNGSFÄHIGKEIT; VERLUST VON NUTZUNGSFÄHIGKEIT; DATEN; PROFIT ODER GESCHÄFTSUNTERBRECHUNG), WIE AUCH IMMER VERURSACHT UND UNTER WELCHER VERPFLICHTUNG AUCH IMMER, OB IN VERTRAG, STRIKTER VERPFLICHTUNG ODER UNERLAUBTE HANDLUNG (INKLUSIVE FAHRLÄSSIGKEIT) VERANTWORTLICH, AUS WELCHEM WEG SIE AUCH IMMER DURCH DIE BENUTZUNG DIESER SOFTWARE ENTSTANDEN SIND, SOGAR, WENN SIE AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS HINGEWIESEN WORDEN SIND.

Hochfrequenzstörungen



Änderungen oder Modifikationen dieses Geräts, die von der für die Konformität verantwortlichen Vertragspartei nicht ausdrücklich genehmigt wurden, können dazu führen, dass die Nutzungsberechtigung für dieses Gerät erlischt.

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.

APC von Schneider Electric, weltweiter Kundendienst

Der Kundendienst für dieses oder jedes andere Produkt steht Ihnen kostenfrei wie folgt zur Verfügung:

- Besuchen Sie die APC-Webseite. Dort können Sie auf die Dokumente der APC Knowledge Base zugreifen und Anfragen an den Kundendienst senden.
  - www.apc.com (Firmensitz)
    Auf der lokalisierten APC-Website des gewünschten Landes können Sie die Informationen des Kundendiensts in der entsprechenden Sprache abrufen.
  - www.apc.com/support/
    Weltweiter Kundendienst über Abfragen der APC Knowledge Base sowie mittels e-Support.
- Wenden Sie sich per Telefon oder E-Mail an den APC-Kundendienst.
  - Lokale, länderspezifische Zentren: Kontaktinformationen finden Sie unter www.apc.com/support/contact.

Wenden Sie sich an die Vertretung oder einen anderen Händler, bei dem Sie Ihr Produkt erworben haben, um zu erfahren, wo Sie Kundendienstunterstützung erhalten können.

© 2019 Schneider Electric. Alle Rechte vorbehalten. Schneider Electric, APC, Network Management Card und Smart-UPS sind Marken und Eigentum von Schneider Electric SE, Tochter- und Beteiligungsgesellschaften. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

990-9996B–005 **5/2019**