

命令行界面指南

UPS Network Management Card 2

AP9630、AP9631、AP9635

990-4879K-037

05/2022

施耐德电气法律免责声明

施耐德电气不保证本手册所提供信息的权威性、正确性或完整性。本出版物并不是要代替详细说明操作步骤的、特定地点专用的开发计划。因此，对于因使用本出版物而导致的损坏、违规、错误安装、系统故障或任何其他问题，施耐德电气不承担任何责任。

本出版物中所包含的信息是按原样提供的，整理这些信息仅用于评估数据中心的设计与结构之目的。本出版物由施耐德电气依照诚信原则编制。然而，本出版物所包含的信息的完整性或准确性未得到任何明示或暗示的说明或担保。

对于因使用或无能力使用本出版物或内容而导致、引发或相关的任何直接、间接、后果性、惩罚性、特殊或连带的损害赔偿（包括但不限于业务、合同、收入、数据、信息损失或业务中断带来的损害赔偿），即使施耐德电气已明确被告知出现此类损害赔偿的可能性，施耐德电气或其任何母公司、子公司或附属公司以及其各自的高管、董事或员工对此不承担任何责任。施耐德电气保留随时更改或更新本出版物内容或其格式的权利，恕不另行通知。

内容（包括但不限于软件、音频、视频、文本和照片）的版权、知识产权以及所有其他专有权利均归施耐德电气或其许可人所有。所有未在此内容中明确授予用户的权利，施耐德电气将予以保留。施耐德电气未向获取此信息的人员授予或分配任何形式的权利，亦不应转让这些权利。

不得以整体或部分形式转售本出版物。

命令行界面 (CLI)

如何登录

概述

若要访问命令行界面，您可以通过本地串行或远程（Telnet 或 SSH）的方式连接到与网络管理卡 (NMC) 处于同一网络的计算机。



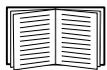
若要访问本 CLI 指南中详细介绍的命令行界面，网络管理卡必须已安装 Smart-UPS 或单相 Symmetra 固件，且网络管理卡必须安装在 Smart-UPS 或单相 Symmetra 型号 UPS 中。有关与网络管理卡兼容的 UPS 型号的详细信息，请参阅 www.apc.com/support 上的知识库文章 [FA237786](#)。

使用区分大小写的用户名和密码登录（默认情况下超级用户或管理员的用户名和密码分别为 **apc** 和 **apc**）。设备用户的默认用户名是 **device**。只读用户不能访问命令行界面。

注意：在 v6.8.0 及更高版本中，首次使用超级用户帐户连接到 NMC 时，系统将提示您输入新密码。

安全锁定。如果有效用户名的密码无效，且连续输入次数达到在 NMC Web 界面中所指定的次数（配置 > 安全 > 本地用户 > 默认设置），设备用户账户将被锁定，直到超级用户或管理员重新启用此账户。

有关这些选项的更多信息，请参阅 [APC](#) 网站上 UPS 网络管理卡 2 的《用户指南》（针对 AP9630、AP9631、AP9635）。



如果您忘记了用户名或密码，请参阅 [APC](#) 网站上《用户指南》中的“如何恢复丢失的密码”。

远程访问命令行界面

您可以通过 Telnet 或 SSH 访问命令行界面。在 v6.8.0 及更高版本中，仅 SSH 默认为启用状态。

若要启用或禁用这些访问方法，请使用 Web 界面。在配置菜单上，选择网络 > 控制台 > 访问。



还可以通过命令行界面启用或禁用 Telnet 或 SSH 访问。请参阅第 13 页上的“console”。

SSH 用于高安全性访问。如果 Web 界面使用安全性较高的 TLS，则可以使用 SSH 访问命令行界面。SSH 会加密用户名、密码和传输的数据。无论是通过 SSH 还是 Telnet 访问命令行界面，界面、用户帐户和用户访问权限都一样，但是要使用 SSH，必须首先配置 SSH 并在计算机上安装 SSH 客户端程序。启用 SSH 的同时还会启用 SCP（安全拷贝），以用于安全文件传输。使用以下示例命令通过 SSH 访问 NMC：

```
ssh -c aes256-ctr apc@156.205.14.141
```

注意：此 SSH 命令适用于 OpenSSH。该命令可能因使用的 SSH 工具而有所不同。

Telnet 用于基本访问。Telnet 通过用户名和密码提供身份验证的基本安全性，但是不具备加密的高安全性优势。

使用 Telnet 访问命令行界面：

1. 在一台能够访问网络且安装了 NMC 的计算机的命令提示符中，键入 telnet NMC 的 IP 地址（例如，当 NMC 使用默认的 Telnet 端口 23 时，地址为 telnet 139.225.6.133），然后按下 ENTER。

注：此示例适用于基于命令提示符的 Telnet 客户端。不同 Telnet 客户端的命令可能有所不同。如果 NMC 使用非默认的端口号（从 5000 到 32768），您必须根据 Telnet 客户端，在 IP 地址（或 DNS 名称）和端口号之间添加冒号或空格。（这些是一般使用的命令：有些客户端不允许您指定端口作为自变量，且某些类型的 Linux 可能需要额外的命令）。

2. 输入用户名和密码。

拨号访问命令行界面（仅限 AP9635）。若要在 AP9635 NMC 上使用调制解调器拨号访问命令行界面：

1. 将有源电话线 (RJ-11) 连接到 AP9635 前面板上的调制解调器端口。
2. 在连接到调制解调器的计算机上，使用调制解调器终端软件（例如，HyperTerminal 或 Tera Term 等第三方终端模拟器程序）拨打为连接到 AP9635 卡的线缆分配的电话号码。
3. 连接时，调制解调器终端软件会打开一个命令行终端。出现提示时，输入用户名和密码。

配置 AP9635 NMC 调制解调器设置

仅可在“配置 INI”文件中进行 AP9635 调制解调器的配置。



有关直接编辑“配置 INI”文件的详细信息，请参阅 [APC](#) 网站上《NMC 用户指南》中的“检索和导出 .ini 文件 - 自定义”。

若要在“配置 INI”文件中配置调制解调器设置：

1. 在文本编辑器中打开“配置 INI”文件
2. 找到标题为 [SystemModem] 的部分，然后更新以下设置：

选项	自变量	说明
ConsoleDialIn	enabled disabled	启用此选项以允许远程调制解调器拨号访问命令行界面。默认情况下为启用状态。
InitString	[AT 命令] [& 命令] [MNP 命令]	InitString 选项接受标准贺氏协议选项。无需编辑 InitString。默认为 [AT&F0E0]。
Country	文本字符串	用于指定连接到 NMC 的有源电话线的拨号号码的国家 / 地区。
DialBack	enabled disabled	启用此选项以指示 NMC 调制解调器在接收到拨号请求时挂断并回拨指定号码。默认情况下，DialBack 为禁用状态。
DialBackString	电话号码	如果已启用 DialBack，此选项为 NMC 接收到拨号请求时要回拨的电话号码。

本地访问命令行界面

对于本地访问，您可以使用通过控制台串行端口连接到**计算机的网络管理卡**访问命令行界面：

1. 选择计算机上的一个串行端口，并禁用使用该端口的所有服务。
2. 将随附的串行缆线（部件号 940-0299）连接到计算机上的选定端口以及 NMC 上的配置端口。
3. 运行终端程序（例如，HyperTerminal、PuTTY 或 Tera Term 等第三方终端模拟器程序），并将选定端口配置为 9600 bps、8 个数据位、无奇偶校验、1 个停止位和无数据流控制。
4. 按下 ENTER。在提示符上，输入用户名和密码。

主屏幕

主屏幕示例

下面是您登录网络管理卡 (NMC) 上的命令行界面时显示的屏幕示例。

```
Schneider Electric                      Network Management Card AOS vx.x.x
(c)Copyright 2019 All Rights Reserved Symmetra APP                          vx.x.x
-----
Name      : Test Lab                      Date : 10/30/2018
Contact   : Don Adams                    Time : 5:58:30
Location  : Building 3                   User  : Super User
Up Time   : 0 Days, 21 Hours, 21 Minutes Stat : P+ N4+ N6+ A+
-----

                          Network Protocols Configuration Summary
-----
Protocol  | Status   | Protocol  | Status   | Protocol  | Status
-----
HTTP      | disabled | HTTPS     | enabled  | FTP       | enabled
Telnet    | disabled | SSH/SFTP  | enabled  | SNMPv1    | enabled
SNMPv3    | disabled | Modbus TCP| enabled  |           |
IPv6      | disabled | IPV4      | enabled  | Ping      | enabled
-----

Type ? for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)

apc>
```

信息和状态字段

主屏幕信息字段

- 以下两个字段表示美国电力转换公司操作系统 (AOS) 和应用程序 (APP) 固件版本。应用程序固件名称表示通过该 NMC 与网络相连的设备。在上面的例子中，NMC 使用 Symmetra UPS 的应用程序固件。

```
Network Management Card AOS    vx.x.x
Symmetra APP                   vx.x.x
```

- 以下三个字段表示系统名称、联系人和 NMC 的位置。（通过在用户界面中选择管理选项卡，在顶部菜单栏中选择常规，然后在左侧导航菜单中选择标识，可设置这些值。）

Name : Test Lab
 Contact : Don Adams
 Location : Building 3

- **Up Time** 字段报告 NMC 管理界面自上次开启或重置以来运行的时长。

Up Time : 0 Days 21 Hours 21 Minutes

- 以下两个字段报告您登录的日期和时间。

Date : 10/30/2018
 Time : 5:58:30

- **User** 字段报告您是通过**超级用户、管理员、设备管理员、仅网络帐户**，还是**只读帐户**登录的。以“设备管理员”（等同于用户界面中的“设备用户”）身份登录时，您可以访问事件日志、配置某些 UPS 设置以及查看活动警报的数量。

User : Super User

主屏幕状态字段

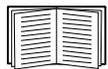
- **Stat** 字段报告 NMC 状态。中间状态会根据您运行的是 IPv4、IPv6 或这两者而变化，详见下面第二个表格。

Stat : P+ N+ A+

P+	操作系统 (AOS) 功能正常。
----	------------------

仅 IPv4	仅 IPv6	IPv4 和 IPv6*	说明
N+	N6+	N4+ N6+	网络功能正常。
N?	N6?	N4? N6?	BOOTP 请求周期正在运行。
N-	N6-	N4- N6-	NMC 未连接到网络。
N!	N6!	N4! N6!	其他设备正在使用 NMC 的 IP 地址。
* N4 和 N6 值可能互不相同：例如，您可以设置 N4- N6+。			

A+	应用程序功能正常。
A-	应用程序校验和错误。
A?	应用程序正在初始化。
A!	应用程序与 AOS 不兼容。



如果未显示 P+，请访问 <http://www.apc.com/site/support/> 联系客户支持。

如何使用命令行界面

概述

使用命令行界面上的诸多选项可以配置网络设置和管理 UPS 及其网络管理卡 (NMC)。

如何输入命令

在命令行界面，使用命令配置 NMC。若要使用某个命令，请键入该命令，并按下 ENTER。命令和自变量可以以小写字母、大写字母或者大小写字母输入。选项区分大小写。

使用命令行界面时，您也可以执行下列操作：

- 键入 `?`，并按下 ENTER，根据您的帐户类型，查看可用的命令。
若要获得有关特定命令的功能和语法信息，请键入该命令、空格和 `?` 或 `help` 字样。例如，若要查看 RADIUS 配置选项，键入：
`radius ?`
或
`radius help`
- 按下向上箭头键可查看当前会话中最近输入的命令。使用向上和向下箭头键可滚动查看最多十个先前输入的命令清单。
- 至少键入某个命令的一个字母，并按下 TAB 键，可翻看与您在命令行键入的文本相匹配的有效命令清单。
- 键入 `ups -st` 可查看 UPS 的状态。
- 键入 `exit` 或 `quit` 可关闭命令行界面的连接。

命令语法

项目	说明
-	选项前面的连字符。
<>	选项的定义包含在尖括号中。例如： <code>-pw < 用户密码 ></code>
[]	如果某个命令接受多个选项或某个选项接受相互独立的自变量，则可以将值包含在括号中。
	包含在括号或尖括号中的项目之间的垂线表示项目之间相互独立。您必须使用其中一个项目。

语法示例

支持多个选项的命令：

```
user -n <用户名> -pw <用户密码>
```

在此，`user` 命令接受指定用户名的选项 `-n`，和更改密码的选项 `-pw`。

例如，要将密码更改为 XYZ，则键入：

```
user -n apc -pw XYZ
```

注： 远程更改密码时，超级用户也需要当前密码。请参阅“User”部分。

选项接受相互独立自变量的命令：

```
alarmcount -p [all | warning | critical]
```

在本示例中，选项 `-p` 只接受三个自变量：`all`、`warning` 或 `critical`。例如，若要查看活动的严重警报数量，键入：

```
alarmcount -p critical
```

如果您键入一个未指定的自变量，该命令无效。

命令响应代码

命令响应代码启用脚本操作，能可靠地检测错误条件，而不必与错误消息文本匹配。

CLI 使用下列格式报告所有命令操作：

```
E [0-9] [0-9] [0-9] : 错误消息
```

代码	错误消息
E000	成功
E001	成功签发
E002	系统需要重新启动，所作的修改方可生效
E100	命令无效
E101	命令未找到
E102	参数错误
E103	命令行错误
E104	用户级拒绝
E105	命令预填
E106	数据不可用
E107	失去与 UPS 的串行通信
E108	由于无效 / 加密的证书，EAPoL 已禁用

命令说明



下列命令和选项的可用性视 UPS 设备而异。

?

使用权限: 超级用户、管理员、设备用户

说明: 查看您的帐户类型可用的所有 CLI 命令清单。若要查看特定命令的帮助文本，请键入该命令和一个问号。

示例: 若要查看 alarmcount 命令接受的选项清单，键入：
alarmcount ?

about

访问权限: 超级用户、管理员、设备用户、仅网络、只读

说明: 查看硬件和固件信息。此信息在故障诊断时很有帮助，您可以用它来确定网站是否有可用的更新固件。

alarmcount

使用权限: 超级用户、管理员、设备用户、只读

说明:

选项	自变量	说明
-p	all	查看 NMC 报告的活动警报的数量。有关警报的信息记录在事件日志中。
	warning	查看活动的警告警报的数量。
	critical	查看活动的严重警报的数量。

示例: 若要查看所有活动的警告警报，键入：
alarmcount -p warning

bacnet

使用权限：超级用户、管理员、设备用户

说明：查看和定义 BACnet 设置。



有关通过 BACnet 提供 UPS 数据点的更多信息，请参阅 [APC](#) 网站上提供的 BACnet 应用程序地图。

选项	自变量	说明
-S	enable disable	选择该选项以启用或禁用 BACnet。如果禁用 BACnet，则不能通过 BACnet 访问 NMC。默认情况下，BACnet 为禁用状态。 注意： 在 v6.8.0 及更高版本中，在设置设备通信控制密码 (-pw) 之前，无法启用 BACnet。
-d	0 - 4194303	此 BACnet 设备的唯一标识符，用于寻址设备。
-n	<device name>	此 BACnet 设备的名称，在 BACnet 网络上必须是唯一的。默认设备名称是 “BACn”+ NMC MAC 地址的最后八位数字。最小长度为 1 个字符，最大长度为 150 个字符，允许使用特殊字符。
-t	1000 - 30000	指定 APDU 超时；NMC 将等待 BACnet 请求响应的毫秒数。缺省值是 6000。
-r	0 - 10	指定 APDU 重试；在中止请求之前，NMC 将做出的 BACnet 请求尝试的数量。缺省值是 3。
-pw	<password>	BACnet 客户端使用设备通信控制服务来命令远程设备（例如，启用了 BACnet 的 NMC）停止发起或停止响应指定持续时间内的所有 APDU（设备通信控制服务除外）。该服务可用于诊断目的。 指定设备通信控制密码，以确保 BACnet 客户端无法控制 NMC 的 BACnet 通信，而无需先提供此处设置的密码。密码必须在 8 到 20 个字符之间，并且必须包含： <ul style="list-style-type: none">• 数字。• 大写字符。• 小写字符。• 特殊字符。 建议在首次启用 BACnet 时更新密码。无需知道当前密码即可更新密码。
BACnet IP 选项：		
-o	47808, 5000 - 65535	指定 NMC 用来发送和接收 BACnet/IP 消息的 UDP/IP 端口。 注： 启用了 BACnet/IP 的 NMC 地址被定义为 NMC 和本地端口的 IP 地址。
-fdre	enable disable	指定启用以使用 BACnet 广播管理设备 (BBMD) 注册 NMC。 注： 如果 NMC 的子网上当前没有 BBMD，或者 NMC 使用不同的本地端口连接到 BBMD，则需要将 NMC 注册为具有 BBMD 的外部设备。有关外部设备注册的更多信息，请参阅 APC 网站 。
-rip	IP address	BACnet 广播管理设备的 IP 地址或完全限定域名 (FQDN)，NMC 卡将在此注册。

选项	自变量	说明
-rpo	5000 - 65535	BBMD 端口，NMC 卡将在此注册。
-fdrttl	1 - 65535	BBMD 将 NMC 保留为注册设备的秒数（生存时间）。如果 NMC 在此时间之前没有重新注册，则 BBMD 将从其外部设备表中删除，NMC 将不再能够通过 BBMD 发送和接收广播消息。

示例：

```

bacnet
E000: Success
Enabled: yes
Device ID: 1013
Device name: BACnB7D7E5F2
Network Protocol: BACnet/IP
APDU timeout (ms): 6000
APDU retries: 3
IP Port: 47808 (0xBAC0)
Registration Enabled: no
Registration Status: Foreign device registration inactive
Registration BBMD: 0.0.0.0
Registration BBMD port: 47808 (0xBAC0)
Registration TTL: 7200

```

boot

访问权限： 超级用户、管理员、仅网络

说明： 定义 NMC 如何获得其网络设置，包括 IP 地址、子网掩码和默认网关。然后配置 BOOTP 或 DHCP 服务器设置。

选项	自变量	说明
-b <启动模式>	dhcp bootp manual	定义开启、重置或重启 NMC 时如何配置 TCP/IP 设置。
-c	enable disable	仅限 dhcp 启动模式。启用或禁用 DHCP 服务器提供 APC cookie 的要求。
-r	1-99	指定 NMC 获取网络设置的频度（以小时为单位）。使用 0 禁用此选项。
-f	always once	定义 NMC 检索 DHCP 引导文件的频度。
这三个设置的默认值一般不需要更改：		
-v	<vendor class>	APC。
-i	<client id>	用于在网上唯一识别 NMC 的 MAC 地址。
-u	<user class>	应用程序固件模块的名称。

示例：若要使用 DHCP 服务器获得网络设置：

1. 键入 `boot -b dhcp`
2. 启用 DHCP 服务器提供 APC cookie 的要求：
`boot -c enable`

bye

访问权限：超级用户、管理员、设备用户、仅网络、只读

说明：从命令行界面会话中退出。这与 `exit` 或 `quit` 命令的作用相同。

示例：

`bye`

Connection Closed - Bye

cd

访问权限：超级用户、管理员、设备用户、仅网络、只读

说明：导航至 NMC 目录结构中的某个文件夹。

示例 1：若要更改为 `ssh` 文件夹，并确认 SSH 安全证书已上传至 NMC：

1. 键入 `cd ssh`，并按下 ENTER。
2. 键入 `dir`，并按下 ENTER，将列出 SSH 文件夹中保存的文件。

示例 2：若要返回先前的目录文件夹，键入：

`cd..`

cipher

访问权限：超级用户、管理员

说明：启用或禁用 Web UI 会话的加密算法。您无法直接从 Web 界面启用或禁用此类算法。启用或禁用算法后，您必须重新启动 NMC，才能使更改生效。

算法分为三类：身份验证算法、分组加密算法和 MAC 算法。另外，还会列出可用和已分组加密包。



禁用类别中的唯一算法会阻止所有 TLS 会话，且 HTTPS 访问可能不会按您的浏览器及其配置运作。

注：在 v6.7.2 及更高版本中，您必须显式启用或禁用算法。

选项	自变量	说明
<code>-aes</code>	<code>enable</code> <code>disable</code>	启用或禁用高级加密标准 (AES)。
<code>-dh</code>	<code>enable</code> <code>disable</code>	启用或禁用 Diffie-Hellman (DH)。
<code>-rsake</code>	<code>enable</code> <code>disable</code>	启用或禁用 RSA 密钥交换。
<code>-rsaau</code>	<code>enable</code> <code>disable</code>	启用或禁用 RSA 身份验证。
<code>-sha1</code>	<code>enable</code> <code>disable</code>	启用或禁用安全哈希算法 1 (SHA-1)。
<code>-sha2</code>	<code>enable</code> <code>disable</code>	启用或禁用安全哈希算法 2 (SHA-2)。
<code>-ecdhe</code>	<code>enable</code> <code>disable</code>	启用或禁用椭圆曲线 Diffie-Hellman 交换 (ECDHE)。

示例：禁用 AES。

```
cipher -aes disable
```

```
E000: Success
```

```
Reboot required for change to take effect.
```

cfgshutdn

使用权限：超级用户、管理员、设备用户

说明：配置关闭参数：您使用它可以显示和配置 UPS 关闭延迟、UPS 恢复延迟、UPS 低电持续时间、UPS 休眠时间、UPS 最低电池电量以及 UPS 最短恢复运行时间。



这些选项并非所有 UPS 设备都提供。

选项	自变量	说明
-all		显示此 UPS 适用的所有关闭参数。
-sd	000 090 180 270 360 450 540 630	设置关闭延迟（单位：秒）。
-lo	02 05 08 11 14 17 20 23	设置低电持续时间（单位：分钟）。
-rd	000 060 120 180 240 300 360 420	设置 UPS 恢复延迟（单位：秒），即 UPS 重新开启前的延迟时间。
-rrt	0-3600	设置最短恢复运行时间（单位：秒），即 UPS 重新开启前电池的运行时间必须达到此值才能支持负载。
-sl	0.0-359.9	设置休眠时间（单位：小时）。自变量可以是 0.0 到 359.9 之间的任意数值。
-rsc	00 15 30 45 60 75 90	设置最低电池电量，以占满电量的百分比表示。

示例：

```
cfgshutdn -all
```

```
E000: Success
```

```
Low Battery Duration: 4 min
```

```
Sleep Time: 0.0 hr
```

cfgpower

使用权限：超级用户、管理员、设备用户

说明：配置电源参数：您使用它可以显示和配置转换点、灵敏度和输出电压。



这些选项并非所有 UPS 设备都提供。

选项	自变量 这些值因不同设备而异。	说明
-all		显示此 UPS 适用的所有电源参数。
-l	97-106	设置低转换点（单位：VAC）。
-h	127-136	设置高转换点（单位：VAC）。
-ov	100 120 110	设置插座电压（单位：VAC）。
-s	Normal Reduced Low	使用这三个自变量之一设置灵敏度。
-bu	127 130 133 136 139 142 145 148	设置旁路电压上限（单位：VAC）；当电压超过此值时，设备将变为旁路。
-bl	086 088 090 092 094 096 098 100	设置旁路电压下限（单位：VAC）；当电压低于此值时，设备将变为旁路。
-rda	Never n+1 n+2	设置在可用冗余电源低于 n+1 或 n+2 时触发的警报。键入 Never，以防止在响应冗余丢失时触发警报。该选项仅适用于 Symmetra 型号 UPS。
-lda	Never 01.0 02.0 03.0 04.0 05.0 06.0 07.0 08.0 09.0 10.0 12.0 14.0 16.0	设置在负载超过指定的 kVA 负载级别时触发的警报。键入 Never，以防止在响应负载级别变更时触发警报。该选项仅适用于 Symmetra 型号 UPS。
-rta	Never 005 010 015 030 045 060 120 180 240 300 360 420 480	设置在可用电池运行时间低于指定分钟数时触发的警报。可用电池运行时间是指 UPS 在电池供电时能够支持当前负载的分钟数。键入 Never，以防止在响应电池运行时间降低时触发警报。该选项仅适用于 Symmetra 型号 UPS。

示例：

```
cfgpower -all
E000: Success
Low Transfer Voltage: 106 VAC
High Transfer Voltage: 127 VAC
Sensitivity: Normal
```

clrrst

使用权限：超级用户、管理员

定义：清除网络接口重置原因。请参阅第 20 页上的“lastrst”。

console

使用权限: 超级用户、管理员、仅网络

说明: 定义用户是使用 Telnet 还是通过以加密形式传输用户名、密码和数据来提供保护的安全接壳 (SSH) 访问命令行界面。为了更加安全, 您可以修改 Telnet 或 SSH 端口的设置。也可以禁用网络对命令行界面的访问。

注意: 在 v6.8.0 及更高版本中, Telnet 默认为禁用状态, 而 SSH 默认为启用状态。

选项	自变量	说明
-s	enable disable	启用或禁用 SSH。启用 SSH 会同时启用 SCP。
-t	enable disable	启用或禁用 Telnet。
-pt	<telnet 端口号 >	指定用于与 NMC 通信的 Telnet 端口号 (默认为 23)。其他范围为 5000–32768。
-ps	<SSH 端口号 >	指定用于与 NMC 通信的 SSH 端口号 (默认为 22)。其他范围为 5000–32768。
-b	2400 9600 19200 38400	配置串行波特率 (默认为 9600)。

示例 1: 若要启用对命令行界面的 Telnet 访问, 键入:

```
console -t
```

示例 2: 若要将 SSH 端口更改为 5000, 键入:

```
console -ps 5000
```

date

使用权限: 超级用户、管理员

定义: 配置 NMC 使用的日期。



若要配置 NTP 服务器, 以为 NMC 定义日期和时间, 请参阅 《用户指南》。

选项	自变量	说明
-d	<“日期字符串”>	设置当前日期。使用 date -f 命令指定的日期格式。
-t	<00:00:00>	配置当前时间的小时、分钟和秒数。使用 24 小时时钟格式。
-f	mm/dd/yy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	选择在该用户界面显示所有日期的数字格式。 每个字母 m (月)、d (日) 和 y (年) 代表一个数位。 单个数位的日和月通过在前面加一个零来表示。
-z	<时区偏移 >	使用格林威治标准时间设置时差, 以便指定您的时区。这样您就可以与不同同时区中的人员保持同步。

示例 1: 若要使用 yyyy-mm-dd 格式显示日期, 键入:

```
date -f yyyy-mm-dd
```

示例 2: 若要使用前一示例中配置的格式将日期定义为 2009 年 10 月 30 日, 键入:

```
date -d "2009-10-30"
```

示例 3: 若要将时间定义为 5:21:03 p.m., 键入:

```
date -t 17:21:03
```

delete

使用权限: 超级用户、管理员

说明: 删除文件系统中的文件。（若要删除事件日志，请参阅《用户指南》。）

自变量	说明
<文件名>	键入要删除的文件的名称。

示例: 若要删除文件:

1. 导航至包含该文件的文件夹。例如，若要导航至 logs 文件夹，键入：
cd logs
2. 若要查看 logs 文件夹中的文件，键入：
dir
3. 键入
delete <文件名>

detbat



该命令并非适用于所有 UPS 设备。

带 SRT 前缀的某些 UPS 设备有不同的选项可供使用。

使用权限: 超级用户、管理员、设备用户

说明: 查看详细的 UPS 电池信息。

选项	自变量	说明
-all	<#>	显示所有电池信息。
-f	<#>	组固件版本。
-t	<#>	组温度。
-pe	<#>	组电池状态。
-s	<#> <#>	组或单元运行状况。
-ph	<#>	电池组运行状况。 注: 此选项仅适用于带有 SRT 前缀的某些 UPS 设备。
-rd	<#> <#>	组或单元的建议更换电池日期。
-pr	<#>	电池组建议更换电池日期。 注: 此选项仅适用于带有 SRT 前缀的某些 UPS 设备。
-id	<#> <#> <"datestring">	组或单元的电池安装日期（以当前日期格式显示）。
-pi	<#> <"datestring">	以当前日期格式显示的电池组安装日期。 注: 此选项仅适用于带有 SRT 前缀的某些 UPS 设备。
-ce	<#> <#>	组或单元电池状态。

示例: `detbat -all`

E000: Success

Firmware Revision (IP): BMC 12.5

Temperature (IP): 26.00C

Pack Status (IP): No Errors

Health (IP, C1): Battery Life OK

Predicted Replacement Date (IP, C1): 07/02/2019

Installation Date (IP, C1): 02/12/2015

Status (IP, C1): OK

detstatus

使用权限: 超级用户、管理员、设备用户

说明: 查看 UPS 的详细状态。另请参阅第 32 页上的“ups”中的 -st 选项。

选项	说明
-all	显示此 UPS 适用的所有状态信息。
-rt	剩余运行时间，以小时和分钟计。
-ss	UPS 状态摘要：市电 / 电池模式等。
-soc	UPS 电池电量，以占满电量的百分比表示。
-om	输出测量值：电压、频率、瓦特百分比、VA 百分比、电流。
-im	输入测量值：电压和频率。
-bat	电池电压。
-tmp	UPS 的内部温度。
-dg	诊断测试结果：自检结果和日期、校准结果和日期。

示例:

`detstatus -rt`

E000: Success

Runtime Remaining: 9 hr 22 min 30 sec

dir

访问权限: 超级用户、管理员、设备用户、仅网络、只读

说明: 查看 NMC 上保存的文件和文件夹。

示例:

```
dir
E000: Success
    3069184 Jun 28 18:07  apc_hw05_aos_664.bin
    3031604 Jul 30 19:05  apc_hw05_sumx_664.bin
    45000 Aug 17 10:54  config.ini
        0 May 14 2018  db/
        0 May 14 2018  ssl/
        0 May 14 2018  ssh/
        0 May 14 2018  logs/
        0 May 14 2018  sec/
        0 May 14 2018  dbg/
        0 May 14 2018  fw1/
        0 May 14 2018  email/
        0 May 14 2018  lang/
        0 May 14 2018  tmp/
        0 May 14 2018  upsfw/
        0 May 14 2018  rms/
        0 May 14 2018  scg/
```

dns

使用权限: 超级用户、管理员

说明: 配置和显示手动域名系统 (DNS) 设置。

选项	自变量	说明
-OM	enable disable	覆盖手动 DNS。
-y	enable disable	同步系统和主机名。 这与使用 “system -s” 的效果一样。
-p	< 主 DNS 服务器 >	设置主 DNS 服务器。
-s	< 次 DNS 服务器 >	设置次 DNS 服务器。
-d	< 域名 >	设置域名。
-n	< 域名 IPv6 >	设置域名 IPv6。
-h	< 主机名 >	设置主机名。

示例:

```
dns -OM
E000: Success
Override Manual DNS Settings: enabled
```

eapol

访问权限: 超级用户、管理员

说明: 配置 EAPoL (802.1X 安全) 设置。

选项	自变量	说明
-S	enable disable	启用或禁用 EAPoL。
-n	<请求者名称>	设置请求者名称。
-p	<私钥密码>	设置私钥密码。

示例 1: 要显示 eapol 命令的结果:

```
apc>eapol
E000: Success
Active EAPoL Settings
-----
Status:enabled
Supplicant Name:NMC-Supplicant Passphrase:<hidden>
CA file Status:Valid Certificate
Private Key Status:Valid Certificate
Public Key Status:Valid Certificate
Result:Success
```

示例 2: 要启用 EAPoL:

```
apc>eapol -S enable
E000: Success
Reboot required for change to take effect.
```

email

使用权限: 超级用户、管理员、仅网络用户

说明: 使用以下命令为 NMC 用来发送事件通知的电子邮件配置参数。

选项	自变量	说明
-g[n]	<enable disable>	启用 (默认) 或禁用发送电子邮件给收件人。
-t[n]	<收件人地址>	收件人的电子邮件地址。

选项	自变量	说明
-o[n]	<long short> (格式)	长格式包含设备名称、位置、联系人、IP 地址、序列号、日期和时间、事件代码以及事件说明。短格式仅提供事件说明。
-l[n]	<语言代码>	发送电子邮件所使用的语言。这取决于安装的语言包。
-r [n]	<Local recipient custom> (路由)	<p>设置 SMTP 服务器选项：</p> <ul style="list-style-type: none"> • Local (建议)：如果您的 SMTP 服务器位于内部网络上，或已设置用于您的电子邮件域，则选择此选项。选择此设置可限制延迟和网络中断。如果选择此设置，您必须同时启用在设备的 SMTP 服务器转发，并设置一个特殊的外部电子邮件帐户来接收转发的电子邮件。注：做出这些更改前，请咨询您的 SMTP 服务器管理员。 • Recipient：此设置可将电子邮件直接发送给收件人的 SMTP 服务器，它由“收件人 :”地址的域 MX 记录查询来确定。设备仅尝试发送电子邮件一次。网络中断或繁忙的远程 SMTP 服务器可能会导致超时，并使电子邮件丢失。此设置无需在 SMTP 服务器上执行其他管理任务。 • Custom：此设置可使每个电子邮件收件人都具有其独有的服务器设置。这些设置不受 -s[n] 选项的设置影响。
-f[n]	<发件人地址>	所发送电子邮件的 发件人 ：字段中由 NMC 使用的发件人电子邮件地址。
-s[n]	<SMTP 服务器>	本地 SMTP 服务器的 IPv4/IPv6 地址或 DNS 名称。如果 -r[n] 选项设置为 Local，则使用此选项。
-p[n]	<端口>	SMTP 端口号，默认为 25。替代端口：465、587、2525、5000 - 32768。
-a[n]	<enable disable> (身份验证)	如果 SMTP 服务器需要进行身份验证，则启用此选项。
-u[n]	<用户名>	如果您的邮件服务器需要身份验证，请在此处键入您的用户名和密码。
-w[n]	<密码>	
-e[n]	<none ifsupported always implicit> (加密)	<ul style="list-style-type: none"> • None：SMTP 服务器不要求也不支持加密。 • If Supported：SMTP 服务器发出支持 STARTTLS 的公告，但不要求加密连接。STARTTLS 命令在发出公告后发送。 • Always：SMTP 服务器要求 STARTTLS 命令在连接到它时发送。 • Implicit：SMTP 服务器只接受已加密的连接。无 STARTTLS 消息发送至服务器。
-c[n]	<enable disable > (所需证书)	此选项只应在您的组织的安全策略不允许 TLS 连接的隐式信任时启用。启用后，必须将有效的根 CA 证书加载到 NMC 才能发送加密电子邮件。
-i[n]	<证书文件名>	此字段取决于 NMC 上安装的根 CA 证书和是否需要根 CA 证书。文件的扩展名必须为 .crt 或 .cer。
n=	电子邮件收件人编号 (1、2、3 或 4)	指定由收件人编号标识的电子邮件收件人。

示例: 若要使用本地 SMTP 服务器将电子邮件发送到地址为 recipient1@apc.com 的收件人 1, 请输入以下内容:

```
email -g1 enable -r1 local -t1 recipient1@apc.com
E000: Success
```

eventlog

访问权限: 超级用户、管理员、设备用户、仅网络、只读

说明: 查看您检索事件日志的日期和时间、UPS 的状态以及连接到 NMC 的传感器的状态。查看最近的设备事件及其发生的日期和时间。使用下列按键导航事件日志:

按键	说明
ESC	关闭事件日志, 并返回命令行界面。
ENTER	更新日志显示。使用该命令可查看您最近检索和显示日志之后记录的事件。
SPACEBAR	查看事件日志的下一页。
B	查看事件日志的上一页。在事件日志的主页面, 该命令不可用。
D	删除事件日志。按照提示, 确认或拒绝删除。删除的事件不可恢复。

exit

访问权限: 超级用户、管理员、设备用户、仅网络、只读

说明: 从命令行界面会话中退出。

firewall

访问权限: 超级用户、管理员、仅网络

说明: 启用、禁用或配置内部 NMC 防火墙功能。

选项	自变量	定义
-S	<enable disable>	启用或禁用防火墙。
-f	< 要激活的文件名 >	要激活的防火墙策略文件的名称。
-t	< 要测试的文件名 >	要测试的防火墙的名称, 持续时间以分钟为单位。
-fe		显示活动文件错误的列表。
-te		显示测试文件错误的列表。
-c		取消防火墙测试。
-r		显示活动防火墙规则的列表。
-l		显示防火墙活动日志。

示例: 若要启用防火墙策略文件 example.fwl, 请输入以下内容:

```
firewall -f example.fwl
E000: Success
```

format

使用权限: 超级用户、管理员

说明: 重新格式化 NMC 的文件系统，并清除所有安全证书、加密密钥、配置设置、事件和数据日志。请谨慎使用该命令。



若要将 NMC 重置为其默认配置，请改用 `resetToDef` 命令。

ftp

访问权限: 超级用户、管理员、仅网络

说明: 启用或禁用对 FTP 服务器的访问。也可以将端口设置更改为 5001 至 32768 之间任何未使用的数字，以增加安全性。

注意: 在 v6.8.0 及更高版本中，FTP 默认为禁用状态。

选项	自变量	定义
-p	< 端口号 >	定义 FTP 服务器用于与 NMC 通信的 TCP/IP 端口（默认为 21）。FTP 服务器使用指定端口和比指定端口低一个号码的端口。
-S	enable disable	配置对 FTP 服务器的访问。

示例: 若要将 TCP/IP 端口更改为 5001，键入：

```
ftp -p 5001
```

help

使用权限: 超级用户、管理员、设备用户、仅网络、只读

说明: 查看您的帐户类型可用的所有 CLI 命令清单。若要查看特定命令的帮助文本，请键入该命令和 `help`。

示例 1: 若要查看以“设备用户”身份登录的用户可用的命令清单，键入：

```
help
```

示例 2: 若要查看 `alarmcount` 命令接受的选项清单，键入：

```
alarmcount help
```

lang

使用权限: 超级用户、管理员、设备用户、只读用户、仅网络用户

说明: 正在使用的语言

示例:

```
lang
```

```
Languages
```

```
enUS - English
```

lastrst

使用权限: 超级用户、管理员

说明: 上次网络接口重置原因。使用此命令的输出可在技术支持部门的指导下对网络接口问题进行故障排除。

示例: lastrst
 09 Coldstart Reset
 E000: Success

ledblink

使用权限: 超级用户、管理员

说明: 将 NMC 的 LED 状态设置为闪烁指定的时间量。使用此命令可帮助视觉定位 NMC。

参数: 时间（单位：分钟）

示例: ledblink 2
 E000: Success

logzip

使用权限: 超级用户、管理员

说明: 为从 NMC 和 UPS 设备提供的日志文件创建单个压缩存档。技术支持部门可使用此类文件解决问题。

选项	自变量	定义
-m	<电子邮件收件人> (电子邮件收件人编号 (1-4))	将 zip 文件发送到的电子邮件收件人的标识编号。输入配置四个可能电子邮件收件人之一的编号。

示例: logzip -m 1
 Generating files
 Compressing files into /dbg/debug_ZA1752123456.tar
 Emailing log files to email recipient - 1
 E000: Success

modbus

使用权限: 超级用户、管理员、设备用户

说明: 查看和配置 Modbus 参数。

选项	自变量	定义
-a	<enable disable> (Modbus 状态)	启用或禁用 Modbus 串口。 ¹
-br	<9600 19200> (波特率)	设置波特率（单位：比特 / 秒）。 ¹
-pr	event odd none	设置奇偶校验位。 ¹
-s	<1-F7> (以十六进制表示的 从属地址)	设置十六进制 Modbus 从属地址。 ¹

选项	自变量	定义
-rDef		将 Modbus 配置重置为默认值。
-tE	<enable disable> (Modbus TCP 状态)	启用或禁用 Modbus TCP。 ²
-tP		指定 Modbus TCP 端口号。默认端口号为 502，可设置为 5000 到 32768 之间的值。 ²
¹ 仅在 AP9635 卡上支持 Modbus 串口。 ² 在 AP9630、AP9631 和 AP9635 卡上支持 Modbus TCP。		

示例: modbus

```
E000: Success
Slave Address = 0x1
Status = ENABLED
Baud Rate = 9600
Parity = none
TCP Status = ENABLED
TCP Port Number = 502
```

netstat

访问权限: 超级用户、管理员、仅网络

说明: 查看网络状态和所有活动的 IPv4 和 IPv6 地址。

示例:

```
netstat

Current IP information

Family  mHome   Type      IP Address                               Status
IPv6    4        auto      FE80::2C0:B7FF:FEEA:D325/64             configured
IPv4    0        manual    10.125.43.115/22                          configured
IPv6    0        manual    ::1/128                                    configured
IPv4    0        manual    127.0.0.1/32                              configured
```

ntp

访问权限: 超级用户、管理员、仅网络

说明: 查看和配置网络时间协议参数。

选项	自变量	定义
-OM	enable disable	覆盖手动设置。
-p	< 主 NTP 服务器 >	指定主服务器。
-s	< 次 NTP 服务器 >	指定次服务器。
-e	enable disable	启用或禁用 NTP。

选项	自变量	定义
-u	<立即更新>	立即通过 NTP 服务器更新 NMC 时间。

示例 1: 若要启用覆盖手动设置功能，键入：

```
ntp -OM enable
```

示例 2: 若要指定主 NTP 服务器，键入：

```
ntp -p 150.250.6.10
```

ping

访问权限: 超级用户、管理员、设备用户、仅网络

说明: 确定使用您指定的 IP 地址或 DNS 名称的设备是否连接至网络。会向地址发送四个查询。

自变量	说明
<IP 地址或 DNS 名称>	使用 xxx.xxx.xxx.xxx 格式键入 IP 地址，或键入 DNS 名称。

示例: 若要确定 IP 地址为 150.250.6.10 的设备是否连接到网络，键入：

```
ping 150.250.6.10
```

portspeed

访问权限: 超级用户、管理员、仅网络

说明:

选项	自变量	说明
-s	auto 10H 10F 100H 100F	定义以太网端口的通信速度。auto 命令使以太网设备能够协商以最高速度传输。

示例: 若要配置 TCP/IP 端口使用 100 Mbps 半双工通信（一次只在一个方向通信），键入：

```
portspeed -s 100H
```

prompt

访问权限: 超级用户、管理员、设备用户、仅网络

说明: 配置命令行界面提示符，包含或排除当前登录的用户的帐户类型。任何用户均可更改此设置；所有用户帐户将会得到更新以使用新设置。

选项	自变量	说明
-s	long	提示符包含当前登录的用户的帐户类型。
	short	提示符长度为四个字符：apc>

示例: 若要在命令提示符中包含当前登录的用户的帐户类型，键入：

```
prompt -s long
```

pwd

使用权限: 超级用户、管理员、设备用户、只读用户、仅网络用户

说明: 用于输出当前工作目录的路径。

quit

访问权限: 超级用户、管理员、设备用户、仅网络、只读

说明: 退出命令行界面会话（这与 `exit` 和 `bye` 命令的作用相同）。

radius

访问权限: 超级用户、管理员、仅网络

说明: 查看现有的 RADIUS 设置、启用或禁用 RADIUS 身份验证以及最多配置两台 RADIUS 服务器的基本身份验证参数。



有关 RADIUS 服务器配置的摘要和支持的 RADIUS 服务器清单，请参阅 [APC](#) 网站上的《用户指南》。

RADIUS 服务器的其他身份验证参数在 NMC 的用户界面上提供。

有关配置 RADIUS 服务器的详细信息，请参阅 [APC](#) 网站上的《安全手册》。

选项	自变量	说明
-a	local radiusLocal radius	配置 RADIUS 身份验证： local — 禁用 RADIUS。启用本地身份验证。 radiusLocal — 先 RADIUS 身份验证，后本地身份验证。启用 RADIUS 和本地身份验证。首先从 RADIUS 服务器请求身份验证。如果 RADIUS 服务器没有响应或无法通过网络来访问，则使用本地身份验证。 radius — 启用 RADIUS。禁用本地身份验证。
-p1 -p2 -o1 -o2	< 服务器 IP >	主或次 RADIUS 服务器的服务器名称或 IP 地址。 注: 默认情况下，RADIUS 服务器使用端口 1812 对用户进行身份验证。若要使用不同的端口，在 RADIUS 服务器名称或 IP 地址末尾添加一个冒号再加上新的端口号。NMC 支持端口 1812、5000 - 32768。
-s1 -s2	< 服务器秘密 >	主或次 RADIUS 服务器与 NMC 之间的共享秘密。
-t1 -t2	< 服务器超时 >	NMC 等待主或次 RADIUS 服务器响应的时间（单位：秒）。

示例 1:

若要查看 NMC 的现有 RADIUS 设置，键入 `radius`，并按下 `ENTER`。

示例 2: 若要启用 RADIUS 和本地身份验证，键入：

```
radius -a radiusLocal
```

示例 3: 若要为次 RADIUS 服务器配置 10 秒超时时间，键入：

```
radius -t2 10
```

reboot

访问权限: 超级用户、管理员、仅网络

说明: 重新启动 NMC 的网络管理界面。



这不会影响安装 NMC 的设备的输出电源。

resetToDef

使用权限: 超级用户、管理员

说明: 将所有可配置参数重置为其默认值。

选项	自变量	说明
-p	all keepip	注意：这会将所有可配置参数重置为其默认值。 重置对配置所作的所有更改，包括事件操作、设备设置以及 TCP/IP 配置设置（可选）。 选择 keepip 可保留用于确定 NMC 如何获取其 TCP/IP 配置值的设置，默认为 DHCP。



某些非可配置参数不可使用 resetToDef 进行重置，且仅可通过使用 **format** 命令格式化文件系统来从 NMC 中清除。

示例: 若要重置对 NMC 的配置所作的所有更改（TCP/IP 设置除外），键入：

```
resetToDef -p keepip
```

session

使用权限: 超级用户、管理员

说明: 记录登录用户、接口、地址、时间和 ID。

选项	自变量	说明
-d	<会话 ID>（删除）	删除具有指定会话 ID 的当前用户会话。
-m	<enable disable> （启用多用户）	启用时，可允许两个或更多个用户同时登录。禁用时，每次只允许一个用户登录。
-a	<enable disable> （远程身份验证覆盖）	NMC 支持在服务器上进行 RADIUS 密码存储。启用“远程身份验证覆盖”可允许本地用户使用存储于本地 NMC 上的用户名和密码登录。

示例:

```
session
```

```
User      Interface  Address          Logged In Time  ID
-----
apc       Telnet    10.169.118.100  00:00:03      19
```

smtp

访问权限: 超级用户、管理员、仅网络

说明: 配置本地电子邮件服务器的设置。

选项	自变量	说明
-f	<发件人地址>	NMC 将从其发送电子邮件的地址。
-s	<SMTP 服务器>	本地 SMTP 服务器的 IPv4/IPv6 地址或 DNS 名称。
-p	<端口>	SMTP 端口号，默认为 25。端口选项包括：25、465、587、2525、5000 - 32768
-a	<enable disable>	如果 SMTP 服务器需要进行身份验证，则启用此选项。
-u	<用户名>	如果 SMTP 服务器需要身份验证，请在此处键入用户名和密码。
-w	<密码>	
-e	<none ifavail always implicit>	加密选项： <ul style="list-style-type: none">• none: SMTP 服务器不要求 / 不支持加密。• ifavail: SMTP 服务器发出支持 STARTTLS 的公告，但不要求加密连接。• always: SMTP 服务器要求 STARTTLS 命令在连接到它时发送。• implicit: SMTP 服务器只接受已加密的连接。无 STARTTLS 消息发送至服务器。

选项	自变量	说明
-c	<enable disable>	需要 CA 根证书： 此选项只应在您组织的安全策略不允许 TLS 连接的隐式信任时启用。启用后，必须将有效的根 CA 证书加载到 NMC 才能发送加密电子邮件。
-i	<证书文件名>	此字段取决于 NMC 上安装的根 CA 证书和是否需要根 CA 证书。

示例：

```

From:      address@example.com
Server:    mail.example.com
Port:      25
Auth:      disabled
User:      User
Password:  <not set>
Encryption: none
Req. Cert: disabled
Cert File: <n/a>

```

snmp

访问权限: 超级用户、管理员、仅网络

说明: 启用或禁用并配置 SNMPv1。

注意: 在 v6.8.0 及更高版本中，SNMPv1 默认为禁用状态。必须设置团体名称 (-c [n])，才能建立 SNMPv1 通信。

在下表中，n 表示访问控制编号：1、2、3 或 4。

选项	自变量	说明
-S	enable disable	启用或禁用 SNMPv1。
-c[n]	团体	指定团体名称或字符串。
-a[n]	read write writeplus disable	指示使用权限。
-n[n]	IP 或域名	指定网络管理站的 IPv4/IPv6 地址或域名。

示例: 若要启用 SNMP 版本 1，键入：

```
snmp -S enable
```

snmpv3

访问权限: 超级用户、管理员、仅网络

说明: 启用或禁用并配置 SNMPv3。

注意: 在 v6.8.0 及更高版本中，SNMPv3 默认为禁用状态。必须使用密码 (-a [n]、-c [n]) 启用有效的用户配置文件，才能建立 SNMPv3 通信。

在下表中， n 表示访问控制编号： 1、 2、 3 或 4。

选项	自变量	说明
-S	enable disable	启用或禁用 SNMPv3。
-u[n]	< 用户名 >	指定用户名、身份验证短语以及加密短语。
-a[n]	< 身份验证短语 >	
-c[n]	< 加密短语 >	
-ap[n]	sha md5 none	指示身份验证协议的类型。
-pp[n]	aes des none	指示隐私（加密）协议。
-ac[n]	enable disable	启用或禁用访问权限。
-au[n]	< 用户配置文件名称 >	授予对指定用户配置文件的访问权限。
-n[n]	<NMS 的 IP 或主机名 >	指定网络管理站的 IPv4/IPv6 地址或主机名。

示例：若要为用户“JMurphy”授予访问级别 2，键入：
snmpv3 -au2 "JMurphy"

snmptrap

使用权限：超级用户、管理员、仅网络用户

说明：启用或禁用 SNMP 陷阱生成。

选项	自变量	说明
-c[n]	< 团体 >	指定团体名称或字符串。
-r[n]	< 接收器 NMS IP >	陷阱接收器的 IPv4/IPv6 地址或主机名。
-l[n]	< 语言 > [语言代码]	指定语言。必须安装包含所需语言的语言包，语言代码如下： <ul style="list-style-type: none"> • enUS - English • deDe - German • ruRu - Russian • zhCn - Chinese • jaJa - Japanese • koKo - Korean • itIt - Italian • ptBr - Portuguese • frFr - French • esEs - Spanish
-t[n]	< 陷阱类型 > [snmpV1 snmpV3]	指定 SNMPv1 或 SNMPv3。
-g[n]	< 生成 > [enable disable]	启用或禁用该陷阱接收器的陷阱生成。默认情况下为启用状态。

选项	自变量	说明
-a[n]	<验证陷阱> [enable disable]	启用或禁用该陷阱接收器的陷阱身份验证（仅限 SNMPv1）。
-u[n]	<profile1 profile2 profile3 profile4> (用户名)	为该陷阱接收器的用户配置文件选择标识符（仅限 SNMPv3）。
n= 陷阱接收器编号 = 1、2、3、4、5 或 6		

示例: 要使用默认语言“英语”针对团体名称为 public、IP 地址为 10.169.118.100 的接收器 1 启用和配置 SNMPv1 陷阱，请输入以下命令：

```
snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1 snmpV1 -g1 enable
E000: Success
```

system

使用权限: 超级用户、管理员

说明: 查看和设置系统名称、联系人、位置，以及查看已运行时间、日期和时间、登录的用户和高层系统状态 P、N、A（请参阅“主屏幕状态字段”）。

选项	自变量	说明
-n	<系统名称>	定义设备名称、设备负责人姓名以及设备的物理位置。 注: 如果您使用多个词定义一个值，则必须将该值用引号引起来。这些值也供 StruxureWare Data Center Expert，或 EcoStruxure IT Expert 和 NMC 的 SNMP 代理使用。
-c	<系统联系人>	
-l	<系统位置>	
-m	<系统消息>	在 Web UI 或 CLI 的登录页上显示自定义消息或横幅。
-s	enable disable	同步系统和主机名。 这与使用“dns -y”的效果一样。

示例 1: 若要将设备位置设置为 Test Lab，键入：

```
system -l "Test Lab"
```

示例 2: 若要将系统名称设置为 Don Adams，键入：

```
system -n "Don Adams"
```

tcpip

访问权限: 超级用户、管理员、仅网络

说明: 查看和手动配置 NMC 的以下 IPv4 TCP/IP 设置：

选项	自变量	说明
-S	enable disable	启用或禁用 TCP/IP v4。
-i	<IP 地址>	使用 xxx.xxx.xxx.xxx 格式键入 NMC 的 IP 地址。

选项	自变量	说明
-s	<子网掩码>	键入 NMC 的子网掩码。
-g	<网关>	键入默认网关的 IP 地址。请勿使用回送地址 (127.0.0.1) 作为默认网关。
-d	<域名>	键入 DNS 服务器配置的 DNS 名称。
-h	<主机名>	键入 NMC 将使用的主机名。

示例 1: 若要查看 NMC 的网络设置，键入 `tcpip`，并按下 ENTER。

示例 2: 若要为 NMC 手动配置 IP 地址 150.250.6.10，键入：
`tcpip -i 150.250.6.10`

tcpip6

访问权限: 超级用户、管理员、仅网络

说明: 启用 IPv6 并查看和手动配置 NMC 的以下 IPv6 TCP/IP 设置：

选项	自变量	说明
-S	enable disable	启用或禁用 TCP/IP v6。
-man	enable disable	启用 NMC 的 IPv6 地址的手动寻址。
-auto	enable disable	允许 NMC 自动配置 IPv6 地址。
-i	<IPv6 地址>	设置 NMC 的 IPv6 地址。
-g	<IPv6 网关>	设置默认网关的 IPv6 地址。
-d6	router statefull stateless never	使用以下参数设置 DHCPv6 模式：由路由器控制、有状态（对于地址和其他信息，都保持其自身的状态）、无状态（对于除地址以外的信息，不保持其自身的状态）和从不。

示例 1: 若要查看 NMC 的网络设置，键入 `tcpip6`，并按下 ENTER。

示例 2: 若要手动配置 NMC 的 IPv6 地址 2001:0:0:0:0:FFD3:0:57ab，键入：
`tcpip -i 2001:0:0:0:0:FFD3:0:57ab`

uio

使用权限: 超级用户、管理员、设备用户

说明: 该命令可用于连接有干触点 I/O 附件 (AP9810) 的 AP9631 或 AP9635 网络管理卡 2。

选项	自变量	说明
-rc <UIO 端口号 >	open close	更改所连接的输出的状态，并指定 UIO (通用输入 / 输出) 端口号。
-st	<UIO · 端口号 <UIO · 端口号 >, <UIO · 端口号 > <UIO · 端口号 >-<UIO · 端口号 >	查看与干触点 I/O 附件相连的传感器的状态。 若要查看特定传感器或多个传感器的状态， 请键入它们的 UIO 端口号。
-disc	<UIO · 端口号 > <UIO · 端口号 >, <UIO · 端口号 > <UIO · 端口号 >-<UIO · 端口号 >	指定新的输入触点或输出继电器连接。

示例 1: 若要打开输出，键入：

```
uio -rc 2 open
```

示例 2: 若要查看连接至通用输入 / 输出端口 2 的干触点 I/O 附件的设备的状态，键入：

```
uio -st 2
```

ups



某些 **ups** 选项取决于 UPS 型号。并非所有配置都支持 **ups** 命令的所有选项。

使用权限: 超级用户、管理员、设备用户

说明：控制 UPS 和查看状态信息。有关与该屏幕相关的这些选项的信息，请参阅 [APC](#) 网站上的《用户指南》。

选项	自变量	说明
-c	reboot	通过下列方式，重新启动连接的装置： <ul style="list-style-type: none"> • 关闭 UPS 电源。 • UPS 电池电量至少恢复为“最低电池电量”中配置的百分比后，打开 UPS 的电源。请参阅“cfgshutdn”。
	on	打开 UPS 的电源。
	off	立即关闭 UPS 的输出电源，没有关机延迟。UPS 将保持关闭状态，直到您再次将其打开。
	graceoff	在“所需的最大延迟”过后，关闭 UPS 的插座电源。
	gracereboot	该操作与上文的重新启动类似，但是在关闭前，有额外的延迟。连接的设备只有在 UPS 等待“所需的最大延迟”后才会关闭，延迟计算方法在《用户指南》的“关闭延迟和 PowerChute Network Shutdown”主题中有介绍。
	sleep	通过在定义的时间内关闭输出电源，使 UPS 进入休眠模式。UPS 在等待“关闭延迟”中配置的时间过后，将关闭输出电源。输入电源恢复时，UPS 在配置的“休眠时间”过后将打开输出电源。请参阅“cfgshutdn”。
	gracesleep	使 UPS 进入休眠模式（在定义的时间内关闭电源）： <ul style="list-style-type: none"> • UPS 在等待“所需的最大延迟”后，关闭输出电源，以确保 PowerChute Network Shutdown 有时间安全地关闭其服务器，并具有充分的“关闭延迟”。 • 输入电源恢复时，UPS 在配置的“休眠时间”过后将打开输出电源。请参阅“cfgshutdn”。
-r	start stop	触发或结束运行时间校准。校准会重新计算剩余的运行时间，并具有下列要求： <ul style="list-style-type: none"> • 由于校准操作会临时消耗 UPS 电池电量，只有电池电量为 100% 时，才可以执行校准。 • 负载必须至少为 15%，才能确保正常进行校准。
-s	start	触发 UPS 自检。
-b	enter exit	控制旁路模式的使用。该命令取决于不同的型号，可能不适用于您的 UPS。

选项	自变量	说明
-o#	Off DelayOff On DelayOn Reboot DelayReboot Shutdown DelayShutdown Cancel	<p>控制 UPS 插座组。使用 # 代替插座组数量。</p> <p>插座组的状态为打开时，该选项接受下列自变量：</p> <ul style="list-style-type: none"> • Off — 立即关闭组。 • DelayOff — 经过关机延迟配置的秒数后，关闭插座组。 • Reboot — 立即关闭组，然后经过重新启动持续时间和供电延迟配置的秒数后将其重新开启。 • DelayReboot — 经过关机延迟配置的秒数后关闭插座组，然后在重新启动持续时间和供电延迟配置的秒数过后将其重新开启。 • Shutdown — 如果 UPS 使用市电模式，这将重新开始插座组。如果 UPS 处于电池模式，这将关闭该组，并在重新开启前等待接通交流市电电源。 • DelayShutdown — 经过关机延迟配置的秒数后，关闭插座组。 • Cancel — 取消之前的命令，例如关闭。 <p>插座组的状态为关闭时，该选项接受两个自变量：</p> <ul style="list-style-type: none"> • On — 立即开启组。 • DelayOn — 经过供电延迟配置的秒数后，开启插座组。 <p>供电延迟、关机延迟和重新启动持续时间必须在用户界面配置。</p>
-os#		<p>查看所有插座组的状态（打开、关闭或重新启动）。</p> <p>若要查看特定插座组的状态，请指定其编号。例如，键入 ups-os1 可查看插座组 1 的状态。</p> <p>但是：</p> <p>a) 当您在带有主插座组的 UPS 上使用此选项时： 1 表示主插座组，2 表示开关插座组 1，3 表示开关插座组 2，依次类推。</p> <p>b) 在不带主插座组的 UPS 上： 1 表示开关插座组 1，依次类推。</p>
-st		查看 UPS 的状态。
-a	start	测试 UPS 的有声警报。

MGE Galaxy 特定的 UPS 设备的 ups 命令选项：



这些命令仅适用于 MGE Galaxy 300 和 MGE Galaxy 7000 UPS。某些选项可能仅适用于个别 UPS 型号。

选项	自变量	说明
-input	<相位编号> all	显示 UPS 选定相的输入测量值。键入“all”显示 UPS 所有相的信息。
	voltage current frequency all	指定 ups 命令的输入测量值。 示例： ups -input 2 frequency 显示 UPS 第 2 相的频率。
-bypass	<相位编号> all	显示旁路市电选定相的输入测量值。键入“all”显示旁路市电的所有相。
	voltage current frequency all	指定 ups 命令的输入测量值。 示例： ups -bypass 2 current 显示旁路市电第 2 相的电流。
-output	<相位编号> all	显示 UPS 选定相的输出测量值。键入“all”显示 UPS 所有相的信息。
	voltage current load power perclload pf frequency all	指定 ups 命令的输出测量值。 示例： ups -output 2 perclload 显示 UPS 第 2 相的负载百分比。
-batt		显示 UPS 的电池状态。
-about		显示有关 UPS 的信息。
-al	c w	显示所有现有的警报。指定“c”或“w”将显示内容限制为“重要”(c)或“警告”(w)警报。

示例 1：若要触发运行时间校准，键入：

```
ups -r start
```

示例 2：若要立即关闭 Smart-UPS XLM 上的插座组 2，键入：

```
ups -o2 off
```

upsabout



upsabout 命令列出的所有 UPS 信息并非适用于所有 UPS 设备。

使用权限: 超级用户、管理员、设备用户。

说明: 显示有关 UPS 的信息，包括：

型号、SKU、序列号、UPS 固件版本、生产日期、表观额定功率、实际额定功率、内部电池 SKU 和外部电池 SKU。

upswupdate



此命令并非适用于所有 UPS 设备。

使用权限: 超级用户、管理员、设备用户。

说明: 启动 UPS 固件更新：



按照 CLI 中的说明来确定是否需要在更新固件之前关闭 UPS 的输出。

- 访问 [APC 网站](#)，阅读 ID 为 [FA164737](#) 和 [FA170679](#) 的知识库文章，了解有关获取固件更新文件的信息。
- 使用 USB 更新（仅限 AP9631 和 AP9635）：
 - USB 驱动器必须支持 USB v1.1，并且格式必须为 FAT、FAT16 或 FAT32。
 - 固件更新文件可保存在 USB 驱动器的根目录或 /upsw/。目录下。
 - 此驱动器必须插入 NMC 的 USB 端口。



注: 固件更新可能需要几分钟时间。UPS 固件更新完成后，才可将 USB 驱动器从 NMC 中移除。如果在更新完成之前移除 USB 驱动器，固件更新将无法成功。

选项	自变量	说明
-install	-file < 文件路径 > -ver < 固件版本 >	<p>注：该选项并非适用于所有 UPS 设备。</p> <p>从插入 NMC USB 端口的 USB 驱动器安装 UPS 固件更新。包括 USB 驱动器上固件更新文件的文件路径。USB 驱动器安装在 NMC 上，驱动器盘符为 C:\。</p> <p>如果 USB 驱动器中有多个固件文件，则以下列格式提供固件版本： [UPS ID 号码] [UPS 固件版本]</p> <p>注：可使用以下介绍的 -info 命令找到 UPS ID 号码。</p>
-info	-file < 文件路径 > -ver < 固件版本 >	<p>从插入 NMC USB 端口的 USB 驱动器中参阅可用固件的相关信息。</p> <p>包括 USB 驱动器上固件更新文件的文件路径。如果 USB 驱动器中有多个固件文件，则以下列格式提供固件版本： [UPS ID 号码] [UPS 固件版本]</p>
-list		显示插入 NMC USB 端口的 USB 驱动器中可用固件版本列表。
-status		检查已启动的固件更新的状态。
-lastresult		查看最近尝试进行固件更新的结果。

示例 1：

```

upsfwupdate -info -ver "ID11 UPS 03.8"
Searching for version 'UPS 03.8'... found.
Version 'UPS 03.8' at C:\SMX11UPS_03-8.enc
E000:Success
Update File:C:\SMX11UPS_03-8.enc
Compatible with UPS:Yes
Update Version:UPS 03.8

```

示例 2：

```

upsfwupdate -status
E000:Success
Status:3k/257k (1%)

```

User

使用权限: 超级用户、管理员

说明: 配置每个帐户类型的用户名和密码，并配置不活动的超时时间。（您无法编辑用户名，您必须将其删除，然后再创建一个新用户）。



有关每个帐户类型（超级用户、管理员、设备用户、只读用户和仅网络用户）的权限信息，请参阅 [APC](#) 网站上的《*用户指南*》。

选项	自变量	说明
-n	< 用户 >	指示用户。
-cp	< 当前密码 >	超级用户必须指定当前密码。 注: 当远程更改“超级用户”的密码时，才需要 -cp 选项。
-pw	< 用户密码 >	指定用户的这些选项。 注: 说明必须用引号括起来。
-pe	< 用户权限 >	
-d	< 用户说明 >	
-e	enable disable	启用或禁用特定用户帐户的访问权限。
-te	enable disable	启用触摸屏访问。
-tp	< 触摸屏访问 pin >	尚不可用。
-tr	enable disable	启用触摸屏远程身份验证覆盖。此选项仅适用于特定设备。如果您启用了此覆盖选项，NMC 将允许本地用户使用存储于本地 NMC 上的密码登录。
-st	< 会话超时 >	指定键盘空闲时注销用户前会话等待的持续时间。
-sr	enable disable	使用串行控制台 (CLI) 连接绕过 RADIUS，也称为串行远程身份验证覆盖
-el	enable disable	指示事件日志颜色编码。
-lf	tab csv	指示导出日志文件的格式。
-ts	us metric	指示温度单位，华氏度或摄氏度。
-df	< mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd >	指定时间格式。
-lg	< 语言代码（如 enUs） >	指定用户语言。键入 lang 以查看所有可用语言。
-del	< 用户名 >	删除用户。
-l		显示当前用户列表。

示例: 若要将用户“JMurphy”的注销时间更改为 10 分钟，键入：

```
user -n "JMurphy" -st 10
```

userdfit

使用权限: 超级用户、管理员

说明: “User” 建立默认用户首选项的补充功能。默认用户设置有两个主要功能:

- 在超级用户或管理员级别帐户创建新用户时，确定要在每个字段中填充的默认值。将设置应用于系统之前，可以更改这些值。
- 对于远程用户（系统中未存储的进行远程身份验证的用户帐户，如 RADIUS），这些是用于身份验证服务器未提供的设置的值。

例如，如果 RADIUS 服务器没有为用户提供温度首选项，则将使用此部分中定义的值。

选项	自变量	定义
-e	<enable disable> (启用)	默认情况下，用户将在创建时启用或禁用。删除末尾的 (启用)。
-pe	<Administrator Device Read-Only Network-Only> (用户权限)	指定用户的权限级别和帐户类型。
-d	<用户说明>	提供用户说明。说明必须用引号括起来。
-st	<会话超时> 分钟	提供默认的会话超时。
-bl	<错误登录尝试>	系统禁用帐户之前用户可进行的错误登录尝试次数。达到此限制后，将会显示一条消息，通知用户帐户已被锁定。超级用户或管理员级别帐户需要重新启用此帐户，该用户才能重新登录。 注: 超级用户帐户无法锁定，但可在需要时手动禁用。
-el	<enable disable> (事件日志颜色编码)	启用或禁用事件日志颜色编码。
-lf	<tab csv> (导出日志格式)	指定日志导出格式: tab 或 CSV。
-ts	<us metric> (温度单位)	指定用户的温度单位。当用户首选项不可用时，此设置也供系统使用 (例如，电子邮件通知)。
-df	<mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd> (日期格式)	指定用户的首选日期格式。

选项	自变量	定义
-lg	<语言代码 (enUs 等) >	指定用户的首选语言。键入 lang 以查看所有可用语言。
-sp	<enable disable>	启用 / 禁用强密码。
-pp	<间隔 (单位: 天) >	所需密码更改间隔。

示例: 若要将默认用户的会话超时设置为 60 分钟, 请输入以下内容:

```
userdfilt -st 60
```

```
E000: Success
```

web

访问权限: 超级用户、管理员、仅网络

说明: 启用使用 HTTP 或 HTTPS 对用户界面的访问。

注意: 在 v6.8.0 及更高版本中, HTTP 默认为禁用状态, 而 HTTPS 默认为启用状态。

为了提高安全性, 您可以将 HTTP 和 HTTPS 的端口设置更改为 5000 - 32768 之间任何未使用的端口。之后, 用户必须在浏览器的地址字段使用冒号 (;) 指定端口号。例如, 对于端口号 5000 和 IP 地址 152.214.12.114, 键入:

```
http://152.214.12.114:5000
```

选项	自变量	定义
-h	enable disable	启用或禁用使用 HTTP 对用户界面的访问。
-hs	enable disable	HSTS (HTTP 严格传输安全协议) 是一种 HTTP 消息头, 用于将不安全的 HTTP 请求重定向到 HTTPS 版本页面。这种方法无需使用不安全的 HTTP 通道, 不容易受到中间人攻击, 因此比简单地使用重定向更安全。 当用户首次访问 NMC 上的 HTTPS 页面时, 该功能会在浏览器中设置严格传输安全消息头, 而且仅当同时启用 HTTP 和 HTTPS 时才可用。该功能可指示浏览器绝不在消息头有效的情况下访问不安全的页面版本。 仅当在 NMC 上加载非自签名证书时, HSTS 才会运行, 因此有必要在 NMC 上加载浏览器信任的证书。
-s	enable disable	启用或禁用使用 HTTPS 对用户界面的访问。 启用 HTTPS 后, 数据在传输过程中将被加密, 并由使用 TLS 的数字证书进行验证。
-mp	<minimum protocol>	指定 Web 界面使用的最低协议版本: TLS v1.1 或 TLS v1.2。
-ph	<http 端口号 >	指定 HTTP 用于与 NMC 通信的 TCP/IP 端口 (默认为 80)。其他范围为 5000-32768。
-ps	<https 端口号 >	指定 HTTPS 用于与 NMC 通信的 TCP/IP 端口 (默认为 443)。其他范围为 5000-32768。
-lsp	enable disable	启用或禁用对 Web UI 中“受限状态”页面的访问。
-lsd	enable disable	在 Web 浏览器中访问设备的 IP 或主机名时, 启用或禁用“受限状态”页面作为默认页面。

示例: 若要禁用使用 HTTPS 对用户界面的一切访问, 键入:

```
web -S disable
```

whoami

使用权限: 超级用户、管理员、仅设备用户、只读用户、仅网络用户

说明: 提供有关当前用户的登录信息

示例:

```
apc> whoami
E000: Success
apc
```

xferINI

使用权限: 超级用户、管理员。该命令仅通过串行 / 本地控制台 CLI 可用。

说明: 您通过串行连接访问命令行界面时，使用 XMODEM 上传 .ini 文件。上传完成后：

- 如果系统或网络有任何更改，命令行界面将重新启动，并且您必须再次登录。
- 如果您选择的文件传输波特率与 NMC 的默认波特率不同，您必须将波特率重置为默认值，才能与 NMC 重新建立通信。

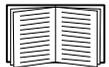
xferStatus

使用权限: 超级用户、管理员

说明: 查看最近文件传输的结果。

示例: xferStatus

```
E000: Success
Result of last file transfer: OK
```



有关传输结果代码的说明，请参阅 [APC](#) 网站上的《*用户指南*》。

版权声明

Cryptlib Cryptology Library

Cryptlib 版权所有 © Digital Data Security New Zealand Ltd 1998。

Berkeley Database

版权所有 © 1991, 1993 The Regents of the University of California。保留所有权利。

如果满足下列条件，则不论是否已修改，都允许以源代码和二进制形式再分发和使用：

1. 源代码的再分发必须保留以上版权声明、此条件列表和以下免责声明。
2. 若以二进制形式再分发，必须在分发时提供的文档和/或其他材料中复制以上版权声明、此条件列表和以下免责声明。
3. 所有提及本软件功能或用途的广告材料必须显示以下确认声明：本产品包含由加州大学伯克利分校 (University of California, Berkeley) 及其贡献者开发的软件。
4. 未经事先书面许可，在本软件基础上开发的产品不得擅用大学名称或其贡献者名称作宣传或促销。

董事会和贡献者“按原样”提供本软件，并特此否认任何明示或暗示的保证，包括但不限于有关适销性和特定用途适用性的暗示保证。在任何情况下，董事会或贡献者对由于使用本软件而造成的任何直接、间接、偶然、特殊、惩罚性或后果性的损失（包括但不限于获得替代商品或服务、无法使用、数据丢失、利润损失或业务中断）不承担任何责任，无论由于什么原因、根据何种责任理由；也无论是否属于合同、严格责任或民事侵权范畴（因疏忽或其他原因），即使事先已被告知可能会造成这种损失，概不例外。

APC by Schneider Electric 全球客户支持

您可以通过以下任意方式免费获得本产品或其他任何产品的客户支持服务：

- 访问 Schneider Electric 网站，以查阅 Schneider Electric 知识库中的文档，以及提交客户支持请求。
 - www.apc.com（公司总部）
连接到特定国家或地区的本地化 Schneider Electric 网站，每个站点均会提供客户支持信息。
 - www.apc.com/support/
通过搜索 Schneider Electric 知识库和使用 e-support 获取全球支持。
- 通过电话或电子邮件联系 Schneider Electric 客户支持中心。
 - 国家 / 地区专属的当地支持中心：有关联系信息，请访问 www.apc.com/support/contact。

有关如何获取当地客户支持的信息，请与客户支持代表或其他向您出售产品的经销商联系。