目 录

1 登录设备方式介绍

设备支持以下登录方式：

- 通过 CLI 登录设备。登录成功后，可以直接输入命令行，来配置和管理设备。CLI 方式下又根据使用的登录接口以及登录协议不同，分为：通过 Console 口、Telnet 或 SSH 登录方式。
- 通过 Web 登录设备。登录成功后，用户可以使用 Web 界面直观地配置和管理网络设备。
- 通过 SNMP 登录设备。登录成功后，NMS 可以通过 Set 和 Get 等操作来配置和管理设备。
- 通过 RESTful 登录设备。登录成功后，用户可以使用 RESTful API 来配置和管理设备。

用户首次登录设备时，只能通过 Console 口登录。只有通过 Console 口登录到设备，进行相应的配置后，才能通过其他方式登录。

说明

此处设备登录方式设置均假设设备启动后不进入自动配置程序。

2 通过Console口首次登录设备

1. 功能简介

通过Console口进行本地登录是登录设备的最基本的方式，也是配置通过其他方式登录设备的基础。

2. 配置准备

在通过 Console 口搭建本地配置环境时，需要通过超级终端或 PuTTY 等终端仿真程序与设备建立连接。用户可以运行这些程序来连接网络设备、Telnet 或 SSH 站点。这些程序的详细介绍和使用方法请参见该程序的使用指导。

3. 配置步骤

通过 Console 口登录设备时，请按照以下步骤进行操作：

(1) 将 PC 断电。

因为 PC 机串口不支持热插拔，请不要在 PC 带电的情况下，将串口线插入或者拔出 PC 机。

(2) 请使用产品随机附带的配置口电缆连接 PC 机和设备。请先将配置口电缆的 DB-9（孔）插头插入 PC 机的 9 芯（针）串口中，再将 RJ-45 插头端插入设备的 Console 口中。

提示

- 连接时请认准接口上的标识，以免误插入其他接口。
- 在拆下配置口电缆时，请先拔出 RJ-45 端，再拔下 DB-9 端。

图2-1 将设备与 PC 通过配置口电缆进行连接

(3) 给 PC 上电。

(4) 打开终端仿真程序，按如下要求设置终端参数：

- 波特率：9600
- 数据位：8
- 停止位：1
- 奇偶校验：无
- 流量控制：无

(5) 设备上电。

在设备自检结束后，用户可通过键入回车进入命令交互界面。出现命令行提示符后即可键入命令来配置设备或查看设备运行状态，需要帮助可以随时键入?。

3 配置通过CLI登录设备

3.1 通过CLI登录设备简介

CLI 登录用户的访问行为需要由用户线管理、限制，即网络管理员可以给每个用户线配置一系列参数，比如用户登录时是否需要认证、用户登录后的角色等。当用户通过 CLI 登录到设备的时候，系统会给用户分配一个用户线，登录用户将受到该用户线下配置参数的约束。

3.1.1 用户线简介

1. 用户线类型

设备提供如下类型的用户线：

- Console 用户线：用来管理和监控通过 Console 口登录的用户。
- VTY（Virtual Type Terminal，虚拟类型终端）用户线：用来管理和监控通过 Telnet 或 SSH 登录的用户。

2. 用户线编号

用户线的编号有绝对编号方式和相对编号方式。

- 绝对编号方式

  使用绝对编号方式，可以唯一的指定一个用户线。绝对编号从 0 开始自动编号，每次增长 1，先给所有 Console 用户线编号，然后是所有 VTY 用户线。使用 **display line**（不带参数）可查看到设备当前支持的用户线以及它们的绝对编号。

- 相对编号方式

  相对编号是每种类型用户线的内部编号，表现形式为“用户线类型 编号”。

3. 用户线分配

用户登录时，系统会根据用户的登录方式，自动给用户分配一个当前空闲的、编号最小的某类型的用户线，整个登录过程将受该用户线视图下配置的约束。用户与用户线并没有固定的对应关系：

- 同一用户登录的方式不同，分配的用户线不同。比如用户 A 使用 Console 口登录设备时，将受到 Console 用户线视图下配置的约束；当使用 Telnet 登录设备时，将受到 VTY 用户线视图下配置的约束。
- 同一用户登录的时间不同，分配的用户线可能不同。比如用户本次使用 Telnet 登录设备，设备为其分配的用户线是 VTY 1。当该用户下次再 Telnet 登录时，设备可能已经把 VTY 1 分配给其他 Telnet 用户了，只能为该用户分配其他的用户线。

如果没有空闲的、相应类型的用户线可分配，则用户不能登录设备。

3.1.2 认证方式简介

在用户线下配置认证方式，可以要求当用户使用指定用户线登录时是否需要认证，以提高设备的安全性。设备支持配置如下认证方式：

- 认证方式为 none：表示下次使用该用户线登录时不需要进行用户名和密码认证，任何人都可以登录到设备上，这种情况可能会带来安全隐患。
- 认证方式为 password：表示下次使用该用户线登录时，需要输入密码。只有密码正确，用户才能登录到设备上。配置认证方式为 password 后，请妥善保存密码。
- 认证方式为 scheme：表示下次使用该用户线登录设备时需要进行用户名和密码认证，用户名或密码错误，均会导致登录失败。配置认证方式为 scheme 后，请妥善保存用户名及密码。

认证方式不同，配置不同，具体配置如 表 3-1 所示。

表3-1 不同认证方式下配置任务简介

认证方式	认证所需配置
none	设置登录用户的认证方式为不认证
password	设置登录用户的认证方式为password认证 设置密码认证的密码
scheme	设置登录用户的认证方式为scheme认证 在ISP域视图下为login用户配置认证方法

3.1.3 用户角色简介

用户角色中定义了允许用户配置的系统功能以及资源对象，即用户登录后执行的命令。关于用户角色的详细描述以及配置请参见“基础配置指导”中的“RBAC”。

- 对于 none 和 password 认证方式，登录用户的角色由用户线下的用户角色配置决定。
- 对于 scheme 认证方式，且用户通过 SSH 的 publickey 或 password-publickey 方式登录设备时，登录用户将被授予同名的设备管理类本地用户视图下配置的授权用户角色。
- 对于 scheme 认证方式，非 SSH 登录以及用户通过 SSH 的 password 方式登录设备时，登录用户使用 AAA 认证用户的角色配置。尤其对于远程 AAA 认证用户，如果 AAA 服务器没有下发用户角色且缺省用户角色授权功能处于关闭状态时，用户将不能登录设备。

3.2 CLI登录配置限制和指导

通过 CLI 登录设备时，有以下限制和指导：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 当用户线或用户线类视图下的属性配置为缺省值时，将优先采用配置为非缺省值的视图下的配置。
- 用户线视图下的配置只对该用户线生效。
- 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效。

3.3 配置通过Console口登录设备

3.3.1 功能简介

通过Console口进行本地登录是登录设备的基本方式之一，用户可以使用本地链路登录设备，便于系统维护。如 图 3-1 所示。具体登录步骤，请参见 通过Console口首次登录设备。

图3-1 通过 Console 口登录设备示意图

缺省情况下，通过 Console 口登录时认证方式为 none，可直接登录。登录成功之后用户角色为network-admin。

首次登录后，建议修改认证方式以及其他参数来增强设备的安全性。

3.3.2 配置限制和指导

改变 Console 口登录的认证方式后，新认证方式对新登录的用户生效。

3.3.3 通过Console口登录设备配置任务简介

通过 Console 口登录设备配置任务如下：

(1) 配置通过Console口登录设备的认证方式

- 配置通过Console口登录设备时无需认证（none）
- 配置通过Console口登录设备时采用密码认证（password）
- 配置通过Console口登录设备时采用AAA认证（scheme）

(2) （可选）配置Console口登录方式的公共属性

3.3.4 配置通过Console口登录设备的认证方式

1. 配置通过Console口登录设备时无需认证（none）

(1) 进入系统视图。

```
system-view
```

(2) 进入 Console 用户线或 Console 用户线类视图。

- 进入 Console 用户线视图。

  line console *first-number* [*last-number*]

- 进入 Console 用户线类视图。

  line class console

(3) 设置登录用户的认证方式为不认证。

```
authentication-mode none
```

缺省情况下，用户通过 Console 口登录，认证方式为 **none**。

(4) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

缺省情况下，通过 Console 口登录设备的用户角色为 network-admin。

2. 配置通过Console口登录设备时采用密码认证（password）

(1) 进入系统视图。

system-view

(2) 进入 Console 用户线或 Console 用户线类视图。

- 进入 Console 用户线视图。

  line console *first-number* [*last-number*]

- 进入 Console 用户线类视图。

  line class console

(3) 设置登录用户的认证方式为密码认证。

authentication-mode password

缺省情况下，用户通过 Console 口登录，认证方式为 **none**。

(4) 设置认证密码。

set authentication password { **hash** | **simple** } *string*

缺省情况下，未设置认证密码。

(5) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

缺省情况下，通过 Console 口登录设备的用户角色为 network-admin。

3. 配置通过Console口登录设备时采用AAA认证（scheme）

(1) 进入系统视图。

system-view

(2) 进入 Console 或 Console 用户线类视图。

- 进入 Console 用户线视图。

  line console *first-number* [*last-number*]

- 进入 Console 用户线类视图。

  line class console

(3) 设置登录用户的认证方式为通过 AAA 认证。

authentication-mode scheme

缺省情况下，用户通过 Console 口登录，认证方式为 **none**。

(4) 在 ISP 域视图下为 login 用户配置认证方法。

如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“用户接入与认证配置指导”中的“AAA”。

3.3.5 配置Console口登录方式的公共属性

1. 配置限制和指导

改变 Console 口属性后会立即生效，所以通过 Console 口登录来配置 Console 口属性可能在配置过程中发生连接中断，建议通过其他登录方式来配置 Console 口属性。

若用户需要通过 Console 口再次登录设备，需要改变 PC 机上运行的终端仿真程序的相应配置，使之与设备上配置的 Console 口属性保持一致。否则，连接失败。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 Console 用户线或 Console 用户线类视图。

- 进入 Console 用户线视图。

  line console *first-number* [*last-number*]

- 进入 Console 用户线类视图。

  line class console

(3) 配置用户线的终端属性。

- 在用户线上启动终端服务。

  shell

  缺省情况下，所有用户线的终端服务功能处于开启状态。

  Console 用户线视图下不允许关闭 shell 终端服务。

- 配置终端的显示类型。

  terminal type { **ansi** | **vt100** }

  缺省情况下，终端显示类型为 ANSI。

  建议设备的终端类型与客户端的终端类型都配置为 VT100，或者均配置为 ANSI 的同时保证当前编辑的命令行的总字符数不超过 80。否则客户端的终端屏幕不能正常显示。

- 配置终端屏幕一屏显示的行数。

  screen-length *screen-length*

  缺省情况下，终端屏幕一屏显示的行数为 24 行。

  screen-length 0 表示关闭分屏显示功能。

- 设置历史命令缓冲区大小。

  history-command max-size *value*

  缺省情况下，每个用户的历史缓冲区的大小为 10，即可存放 10 条历史命令。

- 设置用户线的空闲超时时间。

  idle-timeout *minutes* [*seconds*]

  缺省情况下，所有的用户线的超时时间为 10 分钟，如果直到超时时间到达，某用户线一直没有用户进行操作，则该用户线将自动断开。

  超时时间为 0 表示永远不会超时。

(4) 设置终端线路的自动执行的命令。

auto-execute command *command*

缺省情况下，终端线路未设置自动执行命令。

用户登录到终端线路后，设备会自动依次执行 *command*，然后退出当前连接。

Console 用户线/Console 用户线类视图下不支持该命令。

(5) 配置快捷键。

- 配置启动终端会话的快捷键。

  activation-key *character*

  缺省情况下，按<Enter>键启动终端会话。

- 配置中止当前运行任务的快捷键。

  escape-key { *character* | **default** }

  缺省情况下，键入<Ctrl+C>中止当前运行的任务。

- 配置对当前用户线进行锁定并重新认证的快捷键。

  lock-key *key-string*

  缺省情况下，不存在对当前用户线进行锁定并重新认证的快捷键。

3.4 配置通过Telnet登录设备

3.4.1 功能简介

设备可以作为Telnet服务器，以便用户能够Telnet登录到设备进行远程管理和监控。具体配置请参见“3.4.3 配置设备作为Telnet服务器配置”。

设备也可以作为Telnet客户端，Telnet到其他设备，对别的设备进行管理和监控。具体配置请参见“3.4.4 配置设备作为Telnet客户端登录其他设备”。

3.4.2 配置限制和指导

改变 Telnet 登录的认证方式后，新认证方式对新登录的用户生效。

3.4.3 配置设备作为Telnet服务器配置

1. 通过Telnet登录设备配置任务简介

设备作为 Telnet 服务器配置任务如下：

(1) 开启Telnet服务

(2) 配置设备作为 Telnet 服务器时的认证方式

- 配置Telnet登录设备时无需认证（none）
- 配置Telnet登录设备时采用密码认证（password）
- 配置Telnet登录设备时采用AAA认证（scheme）

(3) （可选）配置Telnet服务器发送报文的公共属性

(4) （可选）配置VTY用户线的公共属性

2. 开启Telnet服务

(1) 进入系统视图。

system-view

(2) 开启设备的 Telnet 服务。

telnet server enable

缺省情况下，Telnet 服务处于关闭状态。

3. 配置Telnet登录设备时无需认证（none）

(1) 进入系统视图。

system-view

(2) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

  line vty *first-number* [*last-number*]

- 进入 VTY 用户线类视图。

  line class vty

(3) 设置登录用户的认证方式为不认证。

authentication-mode none

缺省情况下，Telnet 用户的认证方式为 **password**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(4) 配置从当前用户线登录设备的用户角色。

user-role *role-name*

缺省情况下，通过 Telnet 登录设备的用户角色为 network-operator。

4. 配置Telnet登录设备时采用密码认证（password）

(1) 进入系统视图。

system-view

(2) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

  line vty *first-number* [*last-number*]

- 进入 VTY 用户线类视图。

  line class vty

(3) 设置登录用户的认证方式为密码认证。

authentication-mode password

缺省情况下，Telnet 用户的认证方式为 **password。**

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(4) 设置密码认证的密码。

set authentication password { **hash** | **simple** } *password*

缺省情况下，未设置密码认证的密码。

(5) （可选）配置从当前用户线登录设备的用户角色。

user-role *role-name*

缺省情况下，通过 Telnet 登录设备的用户角色为 network-operator。

5. 配置Telnet登录设备时采用AAA认证（scheme）

(1) 进入系统视图。

system-view

(2) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

  line vty *first-number* [*last-number*]

- 进入 VTY 用户线类视图。

  line class vty

(3) 设置登录用户的认证方式为通过 AAA 认证。

authentication-mode scheme

缺省情况下，Telent 用户的认证方式为 **password**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(4) 在 ISP 域视图下为 login 用户配置认证方法。

如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“用户接入与认证配置指导”中的“AAA”。

6. 配置Telnet服务器发送报文的公共属性

(1) 进入系统视图。

system-view

(2) 配置 Telnet 服务器发送报文的 DSCP 优先级。

（IPv4 网络）

telnet server dscp *dscp-value*

（IPv6 网络）

telnet server ipv6 dscp *dscp-value*

缺省情况下，Telnet 服务器发送 Telnet 报文的 DSCP 优先级为 48。

(3) 配置 Telnet 协议的端口号。

（IPv4 网络）

telnet server port *port-number*

（IPv6 网络）

telnet server ipv6 port *port-number*

缺省情况下，Telnet 协议的端口号为 23。

(4) 配置 Telnet 登录同时在线的最大用户连接数。

aaa session-limit telnet *max-sessions*

缺省情况下，Telnet 方式登录同时在线的最大用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。

关于该命令的详细描述，请参见“用户接入与认证命令参考”中的“AAA”。

7. 配置VTY用户线的公共属性

(1) 进入系统视图。

system-view

(2) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

  line vty *first-number* [*last-number*]

- 进入 VTY 用户线类视图。

  line class vty

(3) 设置 VTY 终端属性。

- 设置在终端线路上启动终端服务。

  shell

  缺省情况下，所有用户线的终端服务功能处于开启状态。

- 配置终端的显示类型。

  terminal type { **ansi** | **vt100** }

  缺省情况下，终端显示类型为 ANSI。

- 设置终端屏幕一屏显示的行数。

  screen-length *screen-length*

  缺省情况下，终端屏幕一屏显示的行数为 24 行。

  取值为 0 表示关闭分屏显示功能。

- 设置设备历史命令缓冲区大小。

  history-command max-size *value*

  缺省情况下，每个用户的历史缓冲区大小为 10，即可存放 10 条历史命令。

- 设置 VTY 用户线的空闲超时时间。

  idle-timeout *minutes* [*seconds*]

  缺省情况下，所有的用户线的超时时间为 10 分钟。如果 10 分钟内某用户线没有用户进行操作，则该用户线将自动断开。

  取值为 0 表示永远不会超时。

(4) 配置 VTY 用户线支持的协议。

protocol inbound { **all** | **ssh** | **telnet** }

缺省情况下，设备同时支持 Telnet 和 SSH 协议。

该配置将在用户下次使用该用户线登录时生效。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(5) 设置从用户线登录后自动执行的命令。

auto-execute command *command*

缺省情况下，未配置自动执行命令。

注意

在配置 **auto-execute command** 命令并退出登录之前，要确保可以通过其他 VTY 用户登录并更改配置，以便出现问题后，能删除该配置。

配置自动执行命令后，用户在登录时，系统会自动执行已经配置好的命令，执行完命令后，自动断开用户连接。如果这条命令引发了一个任务，系统会等这个任务执行完毕后再断开连接。

(6) 配置快捷键。

- 配置中止当前运行任务的快捷键。

  escape-key { *key-string* | **default** }

  缺省情况下，键入<Ctrl+C>中止当前运行的任务。

- 配置对当前用户线进行锁定并重新认证的快捷键。

  lock-key *key-string*

  缺省情况下，不存在对当前用户线进行锁定并重新认证的快捷键。

3.4.4 配置设备作为Telnet客户端登录其他设备

1. 功能简介

用户已经成功登录到了设备上，并希望将当前设备作为Telnet客户端登录到Telnet服务器上进行操作，如 图 3-2 所示。

图3-2 通过设备登录到其他设备

2. 配置准备

先配置设备 IP 地址并获取 Telnet 服务器的 IP 地址。如果设备与 Telnet 服务器相连的端口不在同一子网内，请保证两台设备间路由可达。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) （可选）指定设备作为 Telnet 客户端时，发送 Telnet 报文的源 IPv4 地址或源接口。

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

缺省情况下，未指定发送 Telnet 报文的源 IPv4 地址和源接口，使用报文路由出接口的主 IPv4 地址作为 Telnet 报文的源地址。

(3) 退回用户视图。

quit

(4) 设备作为 Telnet 客户端登录到 Telnet 服务器。

（IPv4 网络）

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] [**dscp** *dscp-value*] [**escape** *character*]

（IPv6 网络）

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] [**dscp** *dscp-value*] [**escape** *character*]

3.5 配置通过SSH登录设备

3.5.1 功能简介

用户通过一个不能保证安全的网络环境远程登录到设备时，SSH（Secure Shell，安全外壳）可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

- 设备可以作为SSH服务器，以便用户能够使用SSH协议登录到设备进行远程管理和监控。具体配置请参见“3.5.2 配置设备作为SSH服务器”。
- 设备也可以作为SSH客户端，使用SSH协议登录到别的设备，对别的设备进行管理和监控。具体配置请参见“3.5.3 配置设备作为SSH客户端登录其他设备”。

3.5.2 配置设备作为SSH服务器

以下配置步骤只介绍采用 **password** 方式认证 SSH 客户端的配置方法，**publickey** 方式的配置方法及 SSH 的详细介绍，请参见“安全配置指导”中的“SSH”。

(1) 进入系统视图。

system-view

(2) 开启 SSH 服务器功能。

ssh server enable

缺省情况下，SSH 服务器功能处于关闭状态。

(3) （可选）建立 SSH 用户，并指定 SSH 用户的认证方式。

ssh user *username* **service-type stelnet authentication-type password**

(4) 进入 VTY 用户线或 VTY 用户线类视图。

- 进入 VTY 用户线视图。

  line vty *first-number* [*last-number*]

- 进入 VTY 用户线类视图。

  line class vty

(5) 配 VTY 用户线的认证方式为 scheme 方式。

authentication-mode scheme

缺省情况下，VTY 用户线的认证方式为 **password** 方式。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(6) （可选）配置 VTY 用户线支持的 SSH 协议。

protocol inbound { all | ssh | telnet }

缺省情况下，设备同时支持 Telnet 和 SSH 协议。

本配置将在用户下次使用该用户线登录时生效。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(7) （可选）配置 SSH 方式登录设备时，同时在线的最大用户连接数。

aaa session-limit ssh *max-sessions*

缺省情况下，SSH 方式登录同时在线的最大用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。

(8) （可选）退回系统视图并配置 VTY 用户线的公共属性。

a. 退回系统视图。

quit

b. 配置 VTY 用户线的公共属性。

详细配置请参见“3.4.3 7. 配置VTY用户线的公共属性”。

3.5.3 配置设备作为SSH客户端登录其他设备

1. 功能简介

用户已经成功登录到了设备上，并希望将当前设备作为SSH客户端登录到其他设备上进行操作，如图 3-3 所示。

图3-3 通过设备登录到其他设备

2. 配置准备

先配置设备 IP 地址并获取 SSH 服务器的 IP 地址。如果设备与 SSH 服务器相连的端口不在同一子网内，请配置路由使得两台设备间路由可达。

3. 配置步骤

请在用户视图下执行本命令，配置设备作为 SSH 客户端登录到 SSH 服务器。

（IPv4 网络）

ssh2 *server*

（IPv6 网络）

ssh2 ipv6 *server*

说明

为配合 SSH 服务器，设备作为 SSH 客户端时还可进一步进行其他配置，具体配置请参见“安全配置指导”中的“SSH”。

3.6 通过CLI登录显示和维护

表3-2 CLI 显示和维护

操作	命令	说明
显示用户线的相关信息	**display line** [*num1* | { **console** | **vty** } *num2*] [**summary**]	在任意视图下执行
显示设备作为Telnet客户端的相关配置信息	**display telnet client**	在任意视图下执行
显示当前正在使用的用户线以及用户的相关信息	**display users**	在任意视图下执行
显示设备支持的所有用户线以及用户的相关信息	**display users all**	在任意视图下执行
释放指定的用户线	**free line** { *num1* | { **console** | **vty** } *num2* }	在用户视图下执行 系统支持多个用户同时对设备进行配置，当管理员在维护设备时，其他在线用户的配置影响到管理员的操作，或者管理员正在进行一些重要配置不想被其他用户干扰时，可以使用以下命令强制断开该用户的连接 不能使用该命令释放用户当前自己使用的连接
锁定当前用户线并设置解锁密码，防止未授权的用户操作该线	**lock**	在用户视图下执行 缺省情况下，系统不会自动锁定当前用户线
锁定当前用户线并对其进行重新认证	**lock reauthentication**	在任意视图下执行 缺省情况下，系统不会自动锁定当前用户线并对其进行重新认证 请使用设备登录密码解除锁定并重新登录设备
向指定的用户线发送消息	**send** { **all** | *num1* | { **console** | **vty** } *num2* }	在用户视图下执行

4 配置通过Web登录设备

4.1 通过Web登录设备简介

为了方便用户对网络设备进行配置和维护，设备提供 Web 功能。用户可以通过 PC 登录到设备上，使用 Web 界面直观地配置和维护设备。

设备支持两种 Web 登录方式：

- HTTP 登录方式：HTTP（Hypertext Transfer Protocol，超文本传输协议）用来在 Internet 上传递 Web 页面信息。HTTP 位于 TCP/IP 协议栈的应用层，传输层采用面向连接的 TCP。设备同时支持 HTTP 协议 1.0 和 1.1 版本。
- HTTPS 登录方式：HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（Secure Sockets Layer，安全套接字层）协议的 HTTP 协议。HTTPS 通过 SSL 协议，能对客户端与设备之间交互的数据进行加密，能为设备制定基于证书属性的访问控制策略，提高了数据传输的安全性和完整性，保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备，从而实现了对设备的安全管理。

4.2 Web登录配置限制和指导

如果设备上开启了 Lighttpd Web 服务功能，则需要配置 HTTP/HTTPS 服务的端口号为 80/443 之外的其他端口号。

如果设备只开启了 HTTP 服务，为了增强设备的安全性，HTTPS 服务的端口号也会被自动打开，且在 HTTP 服务开启的状态下无法通过 **undo ip https enable** 命令关闭。

4.3 Web登录配置任务简介

Web 登录配置任务如下：

(1) 配置通过 Web 登录设备

请选择其中一项进行配置：

- 配置通过HTTP方式登录设备
- 配置通过HTTPS方式登录设备

(2) 配置用于Web登录的本地用户

(3) 管理Web登录用户连接

(4) 开启Web操作日志输出功能

4.4 Web登录配置准备

在通过 Web 登录设备前，需要配置设备的 IP 地址，确保设备与 Web 登录用户间路由可达。

4.5 配置通过HTTP方式登录设备

(1) （可选）请在用户视图下执行本命令，配置用户访问 Web 的固定校验码。

web captcha *verification-code*

缺省情况下，用户只能使用 Web 页面显示的校验码访问 Web。

(2) 进入系统视图。

system-view

(3) 开启 HTTP 服务。

ip http enable

缺省情况下，HTTP 服务处于关闭状态。

(4) （可选）配置 HTTP 服务的端口号。

ip http port *port-number*

缺省情况下，HTTP 服务的端口号为 80。

(5) （可选）配置 HTTP 服务在响应 OPTIONS 请求时返回的方法列表。

http method { delete | get | head | options | post | put } *

缺省情况下，未配置任何方法。

4.6 配置通过HTTPS方式登录设备

1. 功能简介

HTTPS 登录方式分为以下两种：

- 简便登录方式：采用这种方式时，设备上只需开启 HTTPS 服务，用户即可通过 HTTPS 登录设备。此时，设备使用的证书为自签名证书，使用的 SSL 参数为各个参数的缺省值。这种方式简化了配置，但是存在安全隐患。（自签名证书指的是服务器自己生成的证书，无需从 CA 获取）
- 安全登录方式：采用这种方式时，设备上不仅要开启 HTTPS 服务，还需要配置 SSL 服务器端策略、PKI 域等。这种方式配置复杂，但是具有更高的安全性。

SSL 的相关描述和配置请参见“安全配置指导”中的“SSL”。PKI 的相关描述和配置请参见“安全配置指导”中的“PKI”。

2. 配置限制和指导

- 更改 HTTPS 服务与 SSL 服务器端的关联策略，需要先关闭 HTTP 和 HTTPS 服务，再重新配置 HTTPS 服务与 SSL 服务器端策略关联，最后重新开启 HTTP 服务和 HTTPS 服务，新的策略即可生效。
- 如需恢复 HTTPS 使用自签名证书的情况，必须先关闭 HTTP 和 HTTPS 服务，再执行 **undo ip https ssl-server-policy**，最后重新开启 HTTP 服务和 HTTPS 服务即可。
- 开启 HTTPS 服务，会触发 SSL 的握手协商过程。在 SSL 握手协商过程中，如果设备的本地证书不存在，则 SSL 协商过程会触发证书申请流程。由于证书申请需要较长的时间，会导致 SSL 协商不成功，从而无法正常启动 HTTPS 服务。此时，需要多次执行 **ip https enable** 命令，HTTPS 服务才能正常启动。

- 如果配置 HTTPS 服务与证书属性访问控制策略关联，则必须同时在与 HTTPS 服务关联的 SSL 服务器端策略中配置 **client-verify enable** 命令，且证书属性访问控制策略中必须至少包括一条 permit 规则，否则任何 HTTPS 客户端都无法登录设备。

3. 配置通过HTTPS方式登录设备

(1) （可选）请在用户视图下执行本命令，配置用户访问 Web 的固定校验码。

web captcha *verification-code*

缺省情况下，用户只能使用 Web 页面显示的校验码访问 Web。

(2) 进入系统视图。

system-view

(3) （可选）配置 HTTPS 服务与其他策略的关联。

- 配置 HTTPS 服务与 SSL 服务器端策略关联。

  ip https ssl-server-policy *policy-name*

  缺省情况下，HTTPS 服务未与 SSL 服务器端策略关联，HTTPS 使用自签名证书。

- 配置 HTTPS 服务与证书属性访问控制策略关联。

  ip https certificate access-control-policy *policy-name*

  缺省情况下，HTTPS 服务未与证书属性访问控制策略关联。

  通过将 HTTPS 服务与已配置的客户端证书属性访问控制策略关联，可以实现对客户端的访问权限进行控制。证书属性访问控制策略的详细介绍请参见“安全配置指导”中的“PKI”。

(4) 开启 HTTPS 服务。

ip https enable

缺省情况下，HTTPS 服务处于关闭状态。

(5) （可选）配置 HTTPS 服务的端口。

ip https port *port-number*

缺省情况下，HTTPS 服务的端口号为 443。

(6) （可选）配置使用 HTTPS 登录设备时的认证方式。

web https-authorization mode { **auto** | **manual** }

缺省情况下，用户使用 HTTPS 登录设备时采用的认证模式为 **manual**。

4.7 配置用于Web登录的本地用户

(1) 进入系统视图。

system-view

(2) 创建本地用户用于 Web 登录，并进入本地用户视图。

local-user *user-name* [**class manage**]

(3) （可选）设置本地用户的密码。

password [{ **hash** | **simple** } *password*]

缺省情况下，不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其他属性验证通过即可认证成功。

(4) 配置 Web 登录用户的属性。

- 配置 Web 登录的用户角色。

  authorization-attribute user-role *user-role*

  缺省情况下，Web 登录的用户角色为 network-operator。
- 配置 Web 登录用户的服务类型。

  service-type { **http** | **https** }

  缺省情况下，未配置用户的服务类型。

4.8 管理Web登录用户连接

1. 配置Web登录用户连接的超时时间

(1) 进入系统视图。

system-view

(2) 配置 Web 登录用户连接的超时时间。

web idle-timeout *minutes*

缺省情况下，Web 闲置超时时间为 10 分钟。

2. 配置同时在线的最大Web用户连接数

(1) 进入系统视图。

system-view

(2) 配置同时在线的最大 Web 用户连接数。

aaa session-limit { **http** | **https** } *max-sessions*

缺省情况下，同时在线的最大 Web 用户连接数为 32。

配置本命令后，已经在线的用户连接不会受到影响，只对新的用户连接生效。如果当前在线的用户连接数已经达到最大值，则新的连接请求会被拒绝，登录会失败。关于该命令的详细描述，请参见“用户接入与认证命令参考”中的“AAA”。

3. 强制在线Web用户下线

请在用户视图下执行本命令，强制在线 Web 用户下线。

free web users { **all** | **user-id** *user-id* | **user-name** *user-name* }

4.9 开启Web操作日志输出功能

(1) 进入系统视图。

system-view

(2) 开启 Web 操作日志输出功能。

webui log enable

缺省情况下，Web 操作日志输出功能处于关闭状态。

4.10 通过Web登录设备显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 Web 用户的信息、HTTP 的状态信息和 HTTPS 的状态信息，通过查看显示信息验证配置的效果；可以在用户视图下执行 **free web users** 命令来强制在线 Web 用户下线。

表4-1 Web 用户显示

操作	命令
显示HTTP的状态信息	**display ip http**
显示HTTPS的状态信息	**display ip https**
显示Web的页面菜单树	**display web menu** [**chinese**]
显示Web用户的相关信息	**display web users**
强制在线Web用户下线	**free web users** { **all** | **user-id** *user-id* | **user-name** *user-name* }

4.11 通过Web登录设备典型配置举例

4.11.1 使用HTTP方式登录设备典型配置举例

1. 组网需求

Host 与 AP 通过 IP 网络相连且路由可达，Host 和 AP 的 IP 地址分别为 192.168.101.99/24 和 192.168.100.99/24。

2. 组网图

图4-1 配置 HTTP 方式登录组网图

3. 配置步骤

创建 VLAN 999，用作远程登录，并将 AP 上与 Host 相连的接口 GigabitEthernet1/0/1 加入 VLAN 999。

```
<AP> system-view
[AP] vlan 999
[AP-vlan999] port gigabitethernet 1/0/1
[AP-vlan999] quit
```

配置 VLAN 999 接口的 IP 地址为 192.168.100.99，子网掩码为 255.255.255.0。

```
[AP] interface vlan-interface 999
[AP-Vlan-interface999] ip address 192.168.100.99 255.255.255.0
[AP-Vlan-interface999] quit
```

配置 Web 用户名为 admin，认证密码为 admin，服务类型为 http，用户角色为 network-admin。

```
[AP] local-user admin
[AP-luser-manage-admin] service-type http
[AP-luser-manage-admin] authorization-attribute user-role network-admin
[AP-luser-manage-admin] password simple admin
[AP-luser-manage-admin] quit
```

配置开启 HTTP 服务。

```
[AP] ip http enable
```

4. 验证配置

在 Host 的浏览器地址栏内输入设备的 IP 地址并回车，浏览器将显示 Web 登录页面。

在“Web 用户登录”对话框中输入用户名及密码，点击<登录>按钮后即可登录，显示 Web 初始页面。成功登录后，用户可以在配置区对设备进行相关配置。

4.11.2 使用HTTPS方式登录设备典型配置举例

1. 组网需求

用户可以通过 Web 页面访问和控制设备。为了防止非法用户访问和控制设备，提高设备管理的安全性，设备要求用户以 HTTPS 的方式登录 Web 页面，利用 SSL 协议实现用户身份验证，并保证传输的数据不被窃听和篡改。

为了满足上述需求，需要进行如下配置：

- 配置 AP 作为 HTTPS 服务器，并为 AP 申请证书。
- 为 HTTPS 客户端 Host 申请证书，以便 AP 验证其身份。

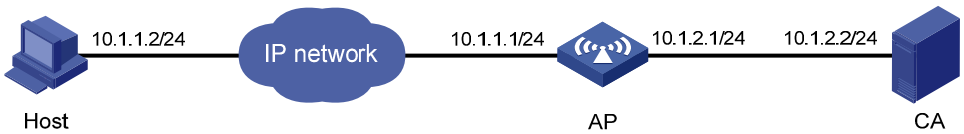
其中，负责为 AP 和 Host 颁发证书的 CA（Certificate Authority，证书颁发机构）名称为 new-ca。

说明

- 本配置举例中，采用 Windows Server 作为 CA。在 CA 上需要安装 SCEP（Simple Certificate Enrollment Protocol，简单证书注册协议）插件。
- 进行下面的配置之前，需要确保 AP、Host、CA 之间路由可达。

2. 组网图

图4-2 HTTPS 配置组网图



3. 配置步骤

(1) 配置 HTTPS 服务器 AP

配置 PKI 实体 en，指定实体的通用名为 http-server1、FQDN 为 ssl.security.com。

```
<AP> system-view
```

```
[AP] pki entity en
[AP-pki-entity-en] common-name http-server1
[AP-pki-entity-en] fqdn ssl.security.com
[AP-pki-entity-en] quit
```

配置 PKI 域 1，指定信任的 CA 名称为 new-ca、注册服务器的 URL 为 http://10.1.2.2/certsrv/mscep/mscep.dll、证书申请的注册受理机构为 RA、实体名称为 en。

```
[AP] pki domain 1
[AP-pki-domain-1] ca identifier new-ca
[AP-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[AP-pki-domain-1] certificate request from ra
[AP-pki-domain-1] certificate request entity en
```

指定证书申请使用的 RSA 密钥对名称为“hostkey”，用途为“通用”，密钥对长度为 1024 比特。

```
[AP-pki-domain-1] public-key rsa general name hostkey length 1024
[AP-pki-domain-1] quit
```

生成本地的 RSA 密钥对。

```
[AP] public-key local create rsa
```

获取 CA 的证书。

```
[AP] pki retrieve-certificate domain 1 ca
```

为 AP 申请证书。

```
[AP] pki request-certificate domain 1
```

创建 SSL 服务器端策略 myssl，指定该策略使用 PKI 域 1，并配置服务器端需要验证客户端身份。

```
[AP] ssl server-policy myssl
[AP-ssl-server-policy-myssl] pki-domain 1
[AP-ssl-server-policy-myssl] client-verify enable
[AP-ssl-server-policy-myssl] quit
```

创建证书属性组 mygroup1，并配置证书属性规则，该规则规定证书颁发者的 DN（Distinguished Name，识别名）中包含 new-ca。

```
[AP] pki certificate attribute-group mygroup1
[AP-pki-cert-attribute-group-mygroup1] attribute 1 issuer-name dn ctn new-ca
[AP-pki-cert-attribute-group-mygroup1] quit
```

创建证书访问控制策略 myacp，并建立控制规则，该规则规定只有由 new-ca 颁发的证书可以通过证书访问控制策略的检测。

```
[AP] pki certificate access-control-policy myacp
[AP-pki-cert-acp-myacp] rule 1 permit mygroup1
[AP-pki-cert-acp-myacp] quit
```

配置 HTTPS 服务与 SSL 服务器端策略 myssl 关联。

```
[AP] ip https ssl-server-policy myssl
```

配置 HTTPS 服务与证书属性访问控制策略 myacp 关联，确保只有从 new-ca 获取证书的 HTTPS 客户端可以访问 HTTPS 服务器。

```
[AP] ip https certificate access-control-policy myacp
```

开启 HTTPS 服务。

```
[AP] ip https enable
```

创建本地用户 usera，密码为 123，服务类型为 https，用户角色为 network-admin。

```
[AP] local-user usera
[AP-luser-usera] password simple 123
[AP-luser-usera] service-type https
[AP-luser-usera] authorization-attribute user-role network-admin
```

(2) 配置 HTTPS 客户端 Host

在 Host 上打开 IE 浏览器，输入网址 http://10.1.2.2/certsrv，根据提示为 Host 申请证书。

4. 验证配置

在 Host 上打开 IE 浏览器，输入网址 https://10.1.1.1，选择 new-ca 为 Host 颁发的证书，即可打开 AP 的 Web 登录页面。在登录页面，输入用户名 usera，密码 123，则可进入 AP 的 Web 配置页面，实现对 AP 的访问和控制。

说明

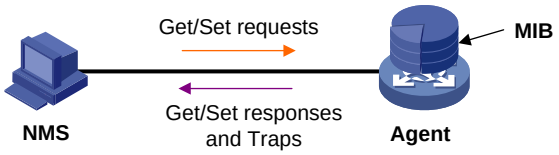
- HTTPS 服务器的 URL 地址以“https://”开始，HTTP 服务器的 URL 地址以“http://”开始。
- PKI 配置命令的详细介绍请参见“安全命令参考”中的“PKI”；
- **public-key local create rsa** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”；
- SSL 配置命令的详细介绍请参见“安全命令参考”中的“SSL”。

---

5 配置通过SNMP登录设备

使用SNMP协议，用户可通过NMS（Network Management System，网络管理系统）登录到设备上，通过Set和Get等操作对设备进行管理、配置，如 图 5-1 所示。

图5-1 通过 SNMP 登录设备组网图



通过 SNMP 登录设备的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

6 对登录用户的控制

6.1 登录用户控制简介

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL 时，允许所有登录用户访问设备；
- 当引用的 ACL 不存在、或者引用的 ACL 为空时，禁止所有登录用户访问设备；

说明

对于 Web 用户，当引用的 ACL 不存在、或者引用的 ACL 为空时，是允许所有 Web 用户访问设备的。

- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其他用户不允许访问设备，以免非法用户访问设备。

关于 ACL 的详细描述和介绍请参见“安全配置指导”中的“ACL”。

用户登录后，可以通过 AAA 功能来对用户使用的命令行进行授权和计费。

6.2 配置对Telnet/SSH用户的控制

6.2.1 配置对Telnet用户的控制

(1) 进入系统视图。

system-view

(2) 配置对 Telnet 用户的访问控制。

（IPv4 网络）

telnet server acl [**mac**] *acl-number*

（IPv6 网络）

telnet server ipv6 acl { **ipv6** | **mac** } *acl-number*

缺省情况下，未对 Telnet 用户进行 ACL 限制。

(3) （可选）开启匹配 ACL deny 规则后打印日志信息功能。

telnet server acl-deny-log enable

缺省情况下，匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

6.2.2 配置对SSH用户的控制

(1) 进入系统视图。

system-view

(2) 配置对 SSH 用户的访问控制。

（IPv4 网络）

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

（IPv6 网络）

ssh server ipv6 acl { **ipv6** { *advanced-acl-number* | *basic-acl-number* } | **mac** *mac-acl-number* }

缺省情况下，未 SSH 用户进行 ACL 限制。

(3) （可选）开启匹配 ACL deny 规则后打印日志信息功能。

ssh server acl-deny-log enable

关于 **ssh server acl**、**ssh server ipv6 acl** 和 **ssh server acl-deny-log enable** 命令的详细介绍请参见“安全命令参考”中的“SSH”。

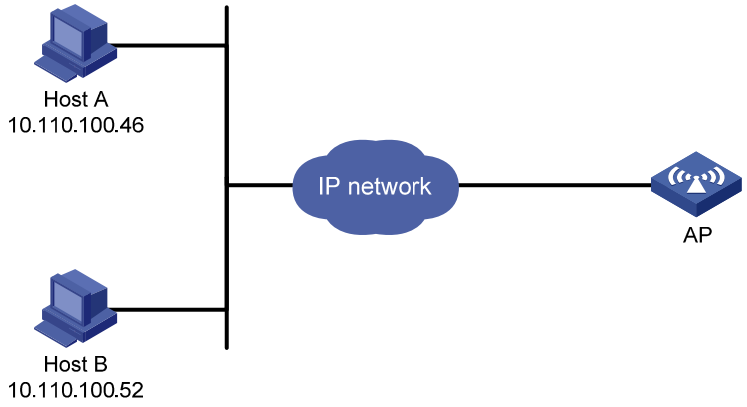
6.2.3 对Telnet用户的控制典型配置举例

1. 组网需求

通过源 IP 对 Telnet 进行控制，仅允许来自 10.110.100.52 的 Telnet 用户访问设备。

2. 组网图

图6-1 使用 ACL 对 Telnet 用户进行控制



3. 配置步骤

定义 ACL。

```
<AP> system-view
[AP] acl basic 2000 match-order config
[AP-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0
[AP-acl-ipv4-basic-2000] quit
```

引用 ACL，允许源地址为 10.110.100.52 的 Telnet 用户访问设备。

```
[AP] telnet server enable
[AP] telnet server acl 2000
```

4. 验证配置

在 Host B（源 IP 地址为 10.110.100.52 的 Telnet 用户）上可以通过 Telnet 方式登录到设备。

```
C:> telnet 10.110.110.66
Trying 10.110.110.66 ...
```

```
Press CTRL+K to abort
Connected to 10.110.110.66 ...

******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<AP>
```

在 Host A 上(源 IP 地址不为 10.110.100.52 的 Telnet 用户)不可以通过 Telnet 方式登录到设备。

```
C:\> telnet 10.110.110.66
Trying 10.110.110.66 ...
Press CTRL+K to abort
Connected to 10.110.110.66 ...
Failed to connect to the remote host!
```

6.3 配置对Web用户的控制

6.3.1 配置通过源IP对Web用户进行控制

(1) 进入系统视图。

system-view

(2) 引用访问控制列表对 Web 用户进行控制。请选择其中一项进行配置。

- 对 HTTP 登录用户进行控制：

  ip http acl [**advanced** | **mac**] { *acl-number* | **name** *acl-name* }

- 对 HTTPS 登录用户进行控制：

  ip https acl [**advanced** | **mac**] {*acl-number* | **name** *acl-name* }

缺省情况下，Web 用户没有引用访问控制列表。

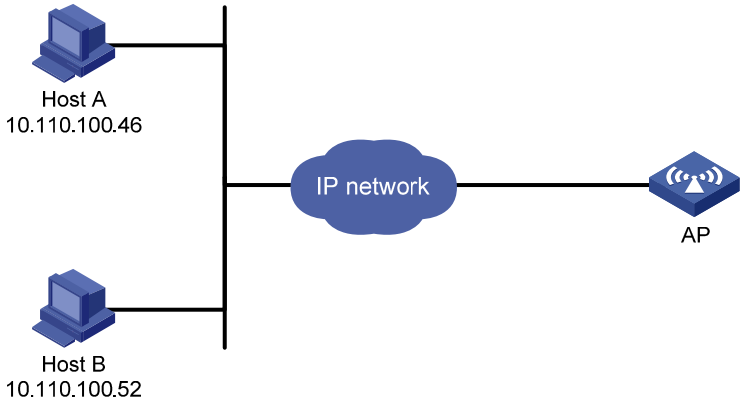
6.3.2 对Web用户的控制典型配置举例

1. 组网需求

通过源 IP 对 Web 用户进行控制，仅允许来自 10.110.100.52 的 Web 用户访问设备。

2. 组网图

图6-2 对 AP 的 HTTP 用户进行 ACL 控制



3. 配置步骤

定义基本访问控制列表。

```
<AP> system-view
[AP] acl basic 2030 match-order config
[AP-acl-ipv4-basic-2030] rule 1 permit source 10.110.100.52 0
```

引用访问控制列表，仅允许来自 10.110.100.52 的 Web 用户访问设备。

```
[AP] ip http enable
[AP] ip http acl 2030
```

4. 验证配置

在 Host B 上打开浏览器，输入 http://10.110.110.66，按下回车，打开 Web 用户登录界面，输入用户名和密码后，按下<登录>按钮，进入设备配置管理 Web 界面。在 Host A 上打开浏览器，输入 http://10.110.110.66，按下回车，打开 Web 用户登录界面，输入用户名和密码后，按下<登录>按钮，无法进入设备配置管理 Web 界面。

6.4 配置对NMS的控制

6.4.1 功能简介

对 NMS 的访问进行控制的详细介绍请参见“网络管理和监控配置指导”中的“SNMP”。

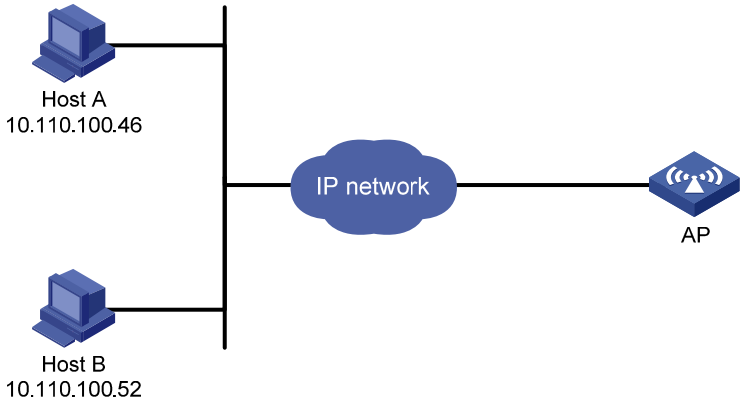
6.4.2 对NMS的控制典型配置举例

1. 组网需求

通过源 IP 对 NMS 进行控制，仅允许来自 10.110.100.52 和 10.110.100.46 的 NMS 访问设备。

2. 组网图

图6-3 使用 ACL 对 NMS 进行控制



3. 配置步骤

定义基本 ACL。

```
<AP> system-view
[AP] acl basic 2000 match-order config
[AP-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0
[AP-acl-ipv4-basic-2000] rule 2 permit source 10.110.100.46 0
[AP-acl-ipv4-basic-2000] quit
```

引用 ACL，仅允许来自 10.110.100.52 和 10.110.100.46 的 NMS 访问设备。

```
[AP] snmp-agent
[AP] snmp-agent community read aaa acl 2000
[AP] snmp-agent group v2c groupa acl 2000
[AP] snmp-agent usm-user v2c usera groupa acl 2000
```

4. 验证配置

在源 IP 地址为 10.110.100.52 或 10.110.100.46 的 NMS 上，可以访问设备；在源 IP 地址不为 10.110.100.52 或 10.110.100.46 的 NMS 上，无法访问设备。

6.5 配置命令行授权功能

6.5.1 功能简介

缺省情况下，用户登录设备后可以使用的命令行由用户拥有的用户角色决定。当用户线采用 AAA 认证方式并配置命令行授权功能后，用户可使用的命令行将受到用户角色和 AAA 授权的双重限制。用户每执行一条命令都会进行授权检查，只有授权成功的命令才被允许执行。

6.5.2 配置限制和指导

要使配置的命令行授权功能生效，还需要在 ISP 域视图下配置命令行授权方法。命令行授权方法可以和 login 用户的授权方法相同，也可以不同。相关详细介绍请参见“用户接入与认证配置指导”中的“AAA”。

6.5.3 配置步骤

(1) 进入系统视图。

system-view

(2) 进入用户线/用户线类视图。请选择其中一项进行配置。

- 进入用户线视图。

  line { *first-number1* [*last-number1*] | { **console** | **vty** } *first-number2* [*last-number2*] }

- 进入用户线类视图。

  line class { **console** | **vty** }

用户线视图下的配置优先于用户线类视图下的配置。用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。用户线类视图下的配置修改会在用户下次登录后生效。

(3) 设置登录用户的认证方式为通过 AAA 认证。

authentication-mode scheme

缺省情况下，用户通过 Console 口登录，认证方式为 **none**；用户通过 VTY 用户线登录，认证方式为 **password**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(4) 开启命令行授权功能。

command authorization

缺省情况下，命令行授权功能处于关闭状态，即用户登录后执行命令行不需要授权。

如果用户类视图下开启了命令行授权功能，则该类型用户线视图都开启命令行授权功能，并且在该类型用户线视图下将无法关闭命令行授权功能。

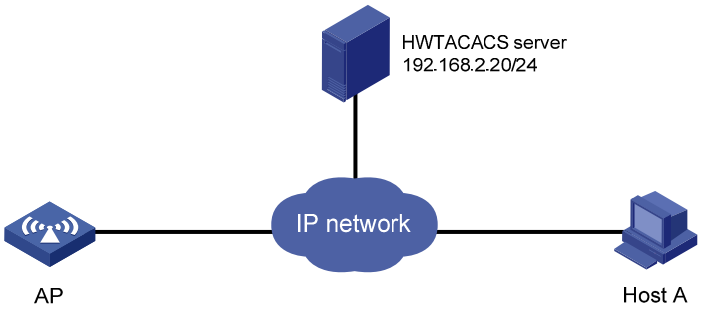
6.5.4 命令行授权典型配置举例

1. 组网需求

为了保证 AP 的安全，需要对登录用户执行命令的权限进行限制：用户 Host A 登录设备后，输入的命令必须先获得 HWTACACS 服务器的授权，才能执行。否则，不能执行该命令。如果 HWTACACS 服务器故障导致授权失败，则采用本地授权。

2. 组网图

图6-4 命令行授权配置组网图



3. 配置步骤

在 AP 上配置 IP 地址，以保证 AP 和 Host A、AP 和 HWTACACS server 之间互相路由可达。（配置步骤略）

开启设备的 Telnet 服务器功能，以便用户访问。

```
<AP> system-view
[AP] telnet server enable
```

配置用户登录设备时，需要输入用户名和密码进行 AAA 认证，可以使用的命令由认证结果决定。

```
[AP] line vty 0 63
[AP-line-vty0-63] authentication-mode scheme
```

开启命令行授权功能，限制用户只能使用授权成功的命令。

```
[AP-line-vty0-63] command authorization
[AP-line-vty0-63] quit
```

配置 HWTACACS 方案：授权服务器的 IP 地址、TCP 端口号分别为 192.168.2.20 和 49（该端口号必须和 HWTACACS 服务器上的设置一致），报文的加密密码是 expert，登录时不需要输入域名，使用缺省域。

```
[AP] hwtacacs scheme tac
[AP-hwtacacs-tac] primary authentication 192.168.2.20 49
[AP-hwtacacs-tac] primary authorization 192.168.2.20 49
[AP-hwtacacs-tac] key authentication simple expert
[AP-hwtacacs-tac] key authorization simple expert
[AP-hwtacacs-tac] user-name-format without-domain
[AP-hwtacacs-tac] quit
```

配置缺省域的命令行授权 AAA 方案，使用 tac local 方案，即优先使用 HWTACACS 方案，HWTACACS 方案认证失败转为本地认证。

```
[AP] domain system
[AP-isp-system] authentication login hwtacacs-scheme tac local
[AP-isp-system] authorization command hwtacacs-scheme tac local
[AP-isp-system] quit
```

配置本地认证所需参数：创建本地用户 monitor，密码为明文的 123，可使用的服务类型为 telnet，用户角色为 level-1。

```
[AP] local-user monitor
[AP-luser-manage-monitor] password simple 123
```

```
[AP-luser-manage-monitor] service-type telnet
[AP-luser-manage-monitor] authorization-attribute user-role level-1
```

4. 验证配置

在 Host A 上通过 Telnet 方式登录到 AP（IP 地址为 10.110.100.77），登录成功后，执行 **ip http enable** 命令，由于授权失败，提示拒绝访问。

```
C:\> telnet 10.110.100.77
Trying 10.110.100.77 ...
Press CTRL+K to abort
Connected to 10.110.100.77 ...

******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: monitor
Password:
<AP> system-view
System View: return to User View with Ctrl+Z.
[AP] ip http enable
Permission denied.
[AP]
```

在 Host A 上通过 Telnet 方式登录到 AP（IP 地址为 10.110.100.77），登录成功后，执行 **interface** 命令，由于授权成功，命令行执行成功。

```
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1]
```

6.6 配置命令行计费功能

6.6.1 功能简介

当用户线采用 AAA 认证方式并配置命令行计费功能后，系统会将用户执行过的命令记录到 HWTACACS 服务器上，以便集中监视用户对设备的操作。命令行计费功能生效后，如果没有配命令行授权功能，则用户执行的每一条合法命令都会发送到 HWTACACS 服务器上做记录；如果配置了命令行授权功能，则用户执行的并且授权成功的命令都会发送到 HWTACACS 服务器上做记录。

6.6.2 配置限制和指导

要使配置的命令行计费功能生效，还需要在 ISP 域视图下配置命令行计费方法。命令行计费方法、命令行授权方法、login 用户的授权方法可以相同，也可以不同。相关详细介绍请参见“用户接入与认证配置指导”中的“AAA”。

6.6.3 配置步骤

(1) 进入系统视图。

system-view

(2) 进入用户线/用户线类视图。请选择其中一项进行配置。

- 进入用户线视图。

  line { *first-number1* [*last-number1*] | { **console** | **vty** } *first-number2* [*last-number2*] }

- 进入用户线类视图。

  line class { **console** | **vty** }

用户线视图下的配置优先于用户线类视图下的配置。用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。用户线类视图下的配置修改将在用户下次登录后生效。

(3) 设置登录用户的认证方式为通过 AAA 认证。

authentication-mode scheme

缺省情况下，用户通过 Console 口登录，认证方式为 **none**；用户通过 VTY 用户线登录，认证方式为 **password**。

用户线视图下，**authentication-mode** 和 **protocol inbound** 存在关联绑定关系，当两条命令中的任意一条配置了非缺省值，那么另外一条取用户线下的值。

(4) 开启命令行计费功能。

command accounting

缺省情况下，命令行计费功能处于关闭状态。

如果用户类视图下开启了命令行计费功能，则该类型用户线视图都开启命令行计费功能，并且在该类型用户线视图下将无法关闭命令行计费功能。

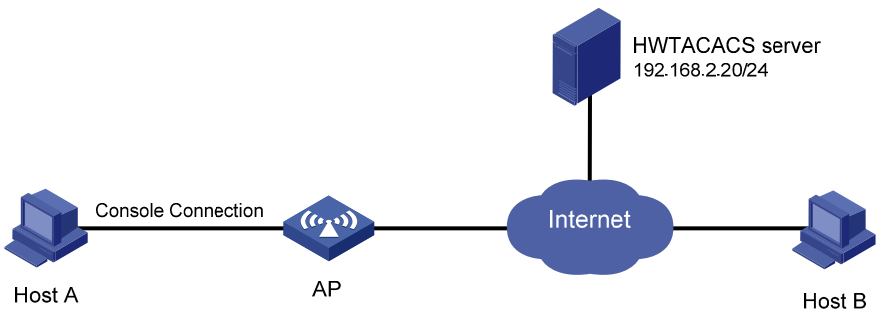
6.6.4 命令行计费典型配置举例

1. 组网需求

为便于集中控制、监控用户对设备的操作，需要将登录用户执行的命令发送到 HWTACACS 服务器进行记录。

2. 组网图

图6-5 命令行计费配置组网图



3. 配置步骤

在 AP 上配置 IP 地址，以保证 AP 和 Host A、Host B、HWTACACS server 路由可达。（配置步骤略）

开启设备的 Telnet 服务器功能，以便用户访问。

```
<AP> system-view
[AP] telnet server enable
```

配置使用 Console 口登录设备的用户执行的命令需要发送到 HWTACACS 服务器进行记录。

```
[AP] line console 0
[AP-line-console0] command accounting
[AP-line-console0] quit
```

配置使用 Telnet 或者 SSH 登录的用户执行的命令需要发送到 HWTACACS 服务器进行记录。

```
[AP] line vty 0 63
[AP-line-vty0-63] command accounting
[AP-line-vty0-63] quit
```

配置 HWTACACS 方案：计费服务器的 IP 地址、TCP 端口号分别为 192.168.2.20 和 49，报文的加密密码是 expert，登录时不需要输入域名，使用缺省域。

```
[AP] hwtacacs scheme tac
[AP-hwtacacs-tac] primary accounting 192.168.2.20 49
[AP-hwtacacs-tac] key accounting simple expert
[AP-hwtacacs-tac] user-name-format without-domain
[AP-hwtacacs-tac] quit
```

配置缺省域的命令行计费 AAA 方案，使用 HWTACACS 方案。

```
[AP] domain system
[AP-isp-system] accounting command hwtacacs-scheme tac
[AP-isp-system] quit
```

4. 验证配置

分别在 Host A、Host B、Host C 上使用 Telnet 方式或者 SSH 方式登录到设备上，进行 VLAN 以及接口下的相关配置，设备向计费服务器发送了计费报文，计费服务器收到报文后，根据用户对计费服务器的配置，对计费报文进行相应处理。