# 18 常见 AAA 操作

## 关于本章

介绍AAA的常见操作。



## 18.1 配置用户通过 Telnet 登录设备的身份认证（AAA 本地认证）

### 背景信息

用户通过Telnet登录设备时，设备上必须配置验证方式，否则用户无法成功登录设备。设备支持不认证、密码认证和AAA认证三种用户界面的验证方式，其中AAA认证方式安全性最高。

采用AAA本地认证方式实现用户通过Telnet登录设备的身份认证，设备上需要开启Telnet服务，将用户界面（以VTY用户界面为例）的验证方式设为aaa，同时在AAA视图下创建本地用户，配置该用户的接入方式和用户级别。

```
<HUAWEI> system-view
[HUAWEI] telnet server enable  //开启Telnet服务
[HUAWEI] user-interface maximum-vty 15  //配置VTY用户界面的登录用户最大数目为15
[HUAWEI] user-interface vty 0 14  //进入0～14的VTY用户界面视图
[HUAWEI-ui-vty0-14] authentication-mode aaa  //配置VTY用户界面的验证方式为aaa
[HUAWEI-ui-vty0-14] protocol inbound telnet  //配置VTY用户界面支持的协议为Telnet，V200R006及之前版本缺省使用的协议为Telnet协议，可以不配置该项；V200R007及之后版本缺省使用的协议为SSH协议，必须配置。
[HUAWEI-ui-vty0-14] quit
[HUAWEI] aaa
```

```
[HUAWEI-aaa] local-user user1 password irreversible-cipher Huawei@1234  //创建本地用户user1并配置密码，由于配置文件中密码以密文显示，建议记住该密码，否则需要重新执行该命令覆盖配置
[HUAWEI-aaa] local-user user1 service-type telnet  //配置本地用户user1的接入类型为Telnet，该用户只能使用Telnet方式登录
[HUAWEI-aaa] local-user user1 privilege level 15  //配置本地用户user1的用户级别为15，该用户登录后可以执行0~15级的命令
[HUAWEI-aaa] quit
```

# 18.2 配置用户级别

用户级别与命令级别相对应，用户登录设备后只能执行命令级别等于或低于自己用户级别的命令，如用户级别为2的用户只能执行命令级别为0，1和2的命令。

用户采用AAA本地认证方式登录设备时，设备上必须配置该用户的用户级别，否则该用户的用户级别为0级（参观级），即用户登录设备后只能执行命令级别为0的命令：**ping**、**tracert**等网络诊断工具命令。如果希望该用户登录设备后可以执行命令级别更高的命令，如监控级、配置级或管理级的命令，用户必须具有更高的用户级别。

当用户的认证方式为AAA本地认证时，可以采用以下方式配置用户级别，**优先级由上到下依次降低**：

- 在AAA视图下配置单个用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user user1 privilege level 15   //配置用户user1的用户级别为15
  ```

- 在业务方案视图下配置某个域下所有用户的用户级别。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] service-scheme sch1
  [HUAWEI-aaa-service-sch1] admin-user privilege level 15   //配置某个域下所有用户的用户级别为15
  ```

- 在用户界面视图下配置从指定用户界面登录的用户的用户级别（以VTY用户界面为例）。缺省情况下，Console口用户界面下用户的级别是15，而VTY用户界面下用户的级别是0。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-interface maximum-vty 15
  [HUAWEI] user-interface vty 0 14
  [HUAWEI-ui-vty0-14] user privilege level 15   //配置VTY 0～VTY 14用户界面下用户级别为15
  ```

**说明**

用户级别为1的用户仍然可以执行配置级命令，可能是因为该级别为用户界面视图下的级别，而设备在业务方案视图或AAA视图下为该用户配置了更大的级别。

# 18.3 配置全局默认域

对于某部门用户，管理员规划其在域“huawei”中进行认证。由于用户认证时提供的用户名经常为不带域名格式，譬如“zhangsan”，这样就导致接入设备无法将用户名上送到在“huawei”域中配置的AAA服务器上进行认证，用户无法通过认证。针对这种情况，可将全局默认域配置为“huawei”。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain huawei
[HUAWEI-aaa-domain-huawei] quit
[HUAWEI-aaa] quit
[HUAWEI] domain huawei
```

  

# 18.4 配置实时计费

实时计费功能有两种配置方法：

- 在设备上通过命令行进行配置：在用户使用的AAA计费方案视图下执行**accounting realtime** *interval*命令开启实时计费功能，并设置实时计费时间间隔。
- 通过RADIUS服务器对认证成功的用户下发RADIUS标准属性**Acct-Interim-Interval**开启实时计费功能，并设置实时计费时间间隔。

## 开启实时计费

上述两种方法选择任一即可开启实时计费功能。同时配置时，RADIUS标准属性**Acct-Interim-Interval**指定的实时计费时间间隔生效。

## 关闭实时计费

如果用户希望关闭实时计费功能，必须同时满足以下条件：

1. 设备上已执行**accounting realtime 0**命令或**undo accounting realtime**命令关闭实时计费功能。
2. RADIUS服务器未对认证成功的用户下发RADIUS标准属性**Acct-Interim-Interval**。
3. 如果RADIUS服务器已对认证成功的用户下发RADIUS标准属性**Acct-Interim-Interval**，则必须在相应的RADIUS服务器模板下执行**radius-attribute disable Acct-Interim-Interval receive send**命令禁用RADIUS标准属性**Acct-Interim-Interval**。

# 18.5 删除本地用户

在AAA视图下执行**undo local-user** *user-name*命令即可删除指定本地用户，包括管理员用户和普通接入用户。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo local-user mike
```

**说明**

本地用户在线时，无法删除。可以等用户不在线时，或在AAA视图下执行**cut access-user username** *user-name*命令切断该用户连接后，再删除该用户。

# 18.6 配置用户连接的超时时间

## 管理用户

对于管理用户，用户登录设备后如果长时间没有进行操作，会造成资源的浪费。此时，可以指定当用户登录设备的时间达到指定数值之后，断开该用户连接。有三种方法：

1. 在用户界面视图下执行**idle-timeout** *minutes* [ *seconds* ]命令配置管理用户连接的超时时间。

  

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] idle-timeout 10
```

2. （仅适用于管理用户的认证方式为AAA本地认证）在AAA视图下执行**local-user** *user-name* **idle-timeout** *minutes* [ *seconds* ]命令配置管理用户连接的超时时间。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain idle-timeout 10
```

3. （仅适用于管理用户的认证方式为RADIUS认证）通过RADIUS服务器为认证成功的用户授权RADIUS属性28（Idle-Timeout），指定管理用户连接的超时时间。

上述三种方法，方法2和方法3的优先级比方法1高。如果方法1和方法2同时配置，方法2生效；如果方法1和方法3同时配置，方法3生效。

## 普通接入用户

对于普通接入用户，用户接入网络后长时间没有访问网络，会造成资源的浪费。此时，可以通过以下两种方法断开普通接入用户的连接：

1. 在设备业务方案视图下执行**idle-cut** *idle-time flow-value*命令，将在超时时间内流量低于指定的流量阈值的用户连接自动断开。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme huawei
[HUAWEI-aaa-service-huawei] idle-cut 1 10
```

2. 通过RADIUS服务器为认证成功的用户授权RADIUS属性28（Idle-Timeout），指定普通接入用户连接的超时时间。

上述两种方法同时配置时，后者生效。

  