

中低端交换机Comware V3和Comware V5设备结合HWTacacs服务器实现命令行授权和计费的配置

一、 案例背景：

在网络设备登录方式多样化的今天，我们可以使用各种方式对设备进行配置和操作，同时如果由于不当的配置导致设备出现了异常，我们一定要通过相关的技术查看是什么人在什么时间点做了什么操作导致了异常的出现，找出事故责任人。那么H3C中低端交换机结合HWTacacs服务器即可完成这一需求。

二、 组网图：

略

三、 配置过程：

- 1) 创建HWTACACS方案，在方案中指定计费服务器的IP地址以及计费过程的其它参数，详细介绍请参见“AAA配置”中的“配置HWTACACS”。
- 2) 在ISP域中引用已创建的HWTACACS方案，详细介绍请参见“AAA配置”中的“配置ISP域的AAA计费方案”。

- 3) 设备使能命令行授权计费功能:

Comware V3设备命令行配置如下

```
[H3C]user-interface vty 0 4
[H3C-ui-vty0-4]authentication-mode scheme command-authorization
[H3C-ui-vty0-4]accounting commands scheme
```

Comware V5设备命令行配置如下

```
[H3C]user-interface vty 0 4
[H3C-ui-vty0-4]authentication-mode scheme
[H3C-ui-vty0-4]command authorization
[H3C-ui-vty0-4]command accounting
```

- 4) HWTacacs服务器具体配置略

四、 配置关键点：

- 1) V3设备通过配置authentication-mode scheme command-authorization命令即可实现用户使用当前用户界面登录设备时结合HWTACACS服务器进行远端用户名和口令的认证功能，并且TACACS认证服务器对不同用户可以使用的命令进行了定义之后，该用户在执行命令时，首先要到TACACS认证服务器上进行命令行授权，只有通过TACACS认证服务器上的命令授权，用户才能执行该命令，否则拒绝用户执行该命令；V5设备则需要配置authentication-mode scheme和command authorization两条命令完成该功能。
- 2) V3设备通过配置accounting commands scheme命令即可实现用户使用当前用户界面登录设备时结合HWTACACS服务器进行远端命令行计费功能。该命令执行成功后，如果没有配置命令行授权功能，则当前用户执行的每一条命令都会发送到HWTACACS服务器上做记录。如果同时也配置了命令行授权功能，则当前用户执行的并且授权成功的命令才会发送到HWTACACS服务器上做记录；V5设备则需要配置command authorization命令完成该功能。