

AR系列路由器使用TACACS+进行telnet登录认证的典型配置

【需求】

要求用户telnet登录时输入用户名huawei和对应的口令huawei123，用户名和口令在TACACS+上验证通过后才能登录路由器。

【配置】

```

配置
#
sysname Quidway
#
hwtacacs nas-ip 192.168.1.254 /设置tacacs+的源地址/
#
hwtacacs scheme test /创建hwtacacs方案/
primary authentication 192.168.1.100 /配置主验证服务器地址/
primary authorization 192.168.1.100 /配置主授权服务器地址/
key authentication huawei /配置认证密钥/
key authorization huawei /配置授权密钥/
user-name-format without-domain /发送账号的格式为不带域名方式/
#
radius scheme system
#
domain system
scheme hwtacacs-scheme test /引用hwtacacs方案“test”/
accounting optional /打开计费可选开关/
#
interface Ethernet1/0/0
ip address 192.168.1.254 255.255.255.0
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme /设置scheme认证/
#
return

```

【验证】

使用huawei/huawei123通过telnet登录系统，该账号密码在TACACS Server上验证通过后，用户才可以登录成功。

【提示】

1. 在tacacs server上创建“huawei/huawei123”的账号口令后，可以使用该账号telnet到路由器；
2. 如果不配置“user-name-format without-domain”，路由器在发送账号的时候会使用huawei@system这种带域名的方式来发送，将导致认证失败；
3. 要确认路由器和tacacs server上的key一致；
4. 对于这种方式只需要对账号进行认证，无需进行计费。所以没有配置计费服务器的参数，并且配置了“accounting optional”来打开计费可选开关；  
当没有可用的计费服务器或与计费服务器通信失败时，若配置了accounting optional命令，则用户可以继续使用网络资源，否则用户将被切断。这个命令经常被用于只认证不计费的情况；
5. 该配置和CISCO ACS 3.1可以正常对接，需要注意在该账号对应的group中给账号进行授权。



