

H3C S5500-SI Telnet用户通过Tacacs进行AAA认证的典型配置

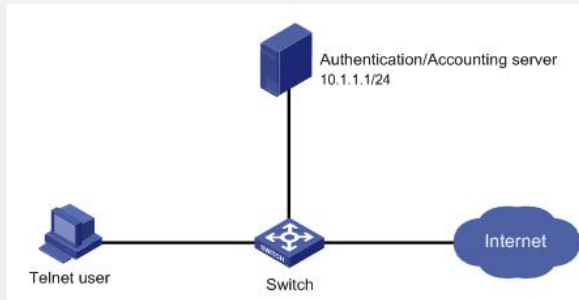
一、组网需求：

通过配置Switch实现HWTACACS服务器对登录Switch的用户进行认证、授权、计费。一台HWTACACS服务器（担当认证、授权、计费服务器的职责）与Switch相连，服务器IP地址为10.1.1.1。

Switch与认证、授权、计费HWTACACS服务器交互报文时的共享密钥均为expert，发送给HWTACACS服务器的用户名中不带域名。

在HWTACACS服务器上设置与Switch交互报文时的共享密钥为expert

二、组网图：



三、配置步骤：

配置各接口的IP地址（略）。

开启Switch的Telnet服务器功能。

```
<Switch> system-view
```

```
[Switch] telnet server enable
```

配置Telnet用户登录采用AAA认证方式。

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

```
[Switch-ui-vty0-4] quit
```

配置HWTACACS方案。

```
[Switch] hwtacacs scheme hwtac
```

```
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```

```
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
```

```
[Switch-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

```
[Switch-hwtacacs-hwtac] key authentication expert
```

```
[Switch-hwtacacs-hwtac] key authorization expert
```

```
[Switch-hwtacacs-hwtac] key accounting expert
```

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
```

```
[Switch-hwtacacs-hwtac] quit
```

配置ISP域的AAA方案。

```
[Switch] domain 1
```

```
[Switch-isp-1] authentication login hwtacacs-scheme hwtac
```

```
[Switch-isp-1] authorization login hwtacacs-scheme hwtac
```

```
[Switch-isp-1] accounting login hwtacacs-scheme hwtac
```

```
[Switch-isp-1] quit
```

或者不区分用户类型，配置缺省的AAA方案。

```
[Switch] domain 1
```

```
[Switch-isp-1] authentication default hwtacacs-scheme hwtac
```

```
[Switch-isp-1] authorization default hwtacacs-scheme hwtac
```

```
[Switch-isp-1] accounting default hwtacacs-scheme hwtac
```

四、配置关键点：

无。