

## 知 telnet 登录125X 进行AAA认证成功后，用户却不能登录设备案例

Telnet 程飞 2016-04-07 发表

S12510X 使用HWTACACS和第三方AAA服务器对接，为telnet登录做验证，服务器侧显示验证通过，但是用户这边一直没办法登录设备，通过debug信息发现验证授权计费全部成功后马上开始了accounting-stop。

```
*Apr 6 10:53:56:839 2016 DC-P-117-B-6-NSW01 TACACS/7/EVENT: PAM_TACACS: Processing accounting reply packet.
```

```
*Apr 6 10:53:56:840 2016 DC-P-117-B-6-NSW01 TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.
```

```
*Apr 6 10:53:56:840 2016 DC-P-117-B-6-NSW01 TACACS/7/EVENT: PAM_TACACS: Processed accounting-stop reply message, resultCode: 0.
```

```
*Apr 6 10:53:56:841 2016 DC-P-117-B-6-NSW01 TACACS/7/EVENT: PAM_TACACS: TACACS stop-accounting succeeded.
```

```
*Apr 6 10:53:56:845 2016 DC-P-117-B-6-NSW01 TELNETD/7/RUN: Successfully closed PTY.
```

由于AAA服务器没下发用户角色，并且设备也没有使能缺省角色导致的。对于通过AAA认证登录设备的用户，由AAA服务器（远程认证）或设备（本地认证）为其授权对应的用户角色。如果用户没有被授权任何用户角色，将无法成功登录设备。缺省用户角色授权功能处于关闭状态，没有被AAA授权用户角色的用户不能登录设备。**role default-role enable**命令用来使能缺省用户角色授权功能。**undo role default-role enable**命令用来恢复缺省情况。

使能缺省用户角色后该功能后，用户将在没有被授权任何用户角色的情况下，具有一个缺省的用户角色，具体情况如下：

如果用户登录于缺省MDC，则缺省用户角色为network-operator；

如果用户登录于非缺省MDC，则缺省用户角色为mdc-operator。

若用户通过AAA认证且被授予了具体的用户角色，则用户不具有以上缺省的用户角色。

1. 需要AAA服务器给用户下发用户角色。
2. 或者需要全局使能：**role default-role enable**