

知 S5560-EI配置端口安全MAC地址认证,给不同终端下发不同授权VLAN问题

徐强 2018-04-11 发表

问题现象：

组网为 S5560-EI——话机——终端（话机注册及话机终端的认证位于认证服务器，相关配置略）

话机和终端都进行MAC认证

测试端口是1/0/10，

其中话机发出的报文自带tag 195 哑终端发出的报文不带tag。

端口使用port-security port-mode mac-authentication

现场期望话机MAC认证成功后下发VLAN 195，终端认证成功后下发 VLAN 185。

目前现场测试结果如下：

如下配置的时候，话机认证成功，终端直连交换机认证成功。但S5560-EI——话机——哑终端时，话机认证成功，终端无法认证成功。

```
interface GigabitEthernet1/0/10
port link-mode bridge
port link-type hybrid
port hybrid vlan 1 195 tagged
port-security port-mode mac-authentication
```

通过打开debugging dot1x all 和 debugging port-security all 排查
终端认证成功后立刻下线。

无

配置port-security port-mode mac-authentication，允许多个终端通过MAC地址认证上线，但这些用户的授权VLAN必须相同，否则只要下发了带tag的VLAN，其他授权VLAN会下发失败，即造成如上问题现象，认证成功但下发授权VLAN失败，终端下线。

在对应端口下配置 mac-vlan enable后，相关授权VLAN下发成功。

在类似使用场景中，对同端口进行MAC认证的多个终端下发不同授权VLAN，需在端口下配置 mac-vlan enable才能保证所有终端的授权VLAN下发成功。