# S5120-EI系列交换机下连PXE客户端无法成功下载系统的解决方法

岳斌 2010-10-21 发表

S5120-EI系列交换机下连PXE客户端无法成功下载系统的解决方法

一、 组网：

PXE客户端直连S5120-EI系列交换机，交换机与软件下载服务器路由可达。

二、 问题描述：

在S5120-EI系列交换机端口上主要配置如下。

```
#
interface GigabitEthernet1/0/2
 port access vlan 10
stp edged-port enable
 port-security port-mode userlogin-secure-ext
 dot1x guest-vlan 10
 dot1x auth-fail vlan 10
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
```

正常情况下，PXE客户端无需认证，待进入VLAN 10（也就是Guest和Authfail VLAN）后自动获得IP并下载操作系统。按照现在的配置， PXE客户端无论是超时不认证还是认证失败都应该进入VLAN 10才对，但是交换机上看不到该端口有MAC地址，而且console上看到提示认证失败并检测到incursion的信息。如下。

```
%Oct 13 17:42:13:826 2010 nhppoc002 PORTSEC/6/PORTSEC_DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/2-MACAddr=00:24:E8:EF:DE:6B-VlanId=10-UserName=NULL; The user failed the 802.1X authentication.
%Oct 13 17:42:14:069 2010 nhppoc002 PORTSEC/5/PORTSEC_VIOLATION: -IfName=GigabitEthernet1/0/2-MACAddr=00:24:E8:EF:DE:6B-VlanId=-10-IfStatus=Up; Intrusion detected.
```

三、 过程分析：

交换机上使用单播报文触发认证时，PXE客户端收到交换机发送的单播报文不会反应，也就是说不会发送用户名和密码，从而无法因为用户名密码错误进入Authfail VLAN，但是交换机在单播触发报文发送后如果没有收到回应报文就会启动认证流程。

此外，Access端口下只存在port-based的Guest VLAN，而port-based的Guest VLAN原理是交换机发送三次组播报文，如果没有客户端响应，则加进Guest VLAN，原有的配置是进行单播触发认证，且端口安全模式为基于MAC的认证，基于MAC的Guest VLAN必须配置hybrid口才能生效，并且需要配置mac-vlan enable命令。因此也就不会因为超时而进入Guest VLAN。

因此，现有配置导致PXE客户端既不会因为超时进入Guest VLAN也不会因为认证失败进入Authfail VLAN，所以才有了上面描述的提示信息。如果可以确认该PXE客户端不需要认证直接进入Guest VLAN，那么可以采用下面方法解决。

四、 解决方法：

正确的配置如下。

```
interface GigabitEthernet1/0/2
 port access vlan 10
stp edged-port enable
 port-security port-mode userlogin
 dot1x guest-vlan 10
 dot1x auth-fail vlan 10
 undo dot1x handshake
```