某局点 S5130S-EI 终端认证后获取地址异常

802.1X MAC地址认证 DHCP/DHCP Relay 倪民 2022-03-07 发表

组网及说明

不涉及

问题描述

1、终端所在接口配置如下

```
interface GigabitEthernet2/0/33
port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
storm-constrain broadcast ratio 70 50
storm-constrain multicast ratio 70 50
stp edged-port
undo dot1x handshake
dot1x mandatory-domain corplink
undo dot1x multicast-trigger
dot1x unicast-trigger
dot1x guest-vlan 500
dot1x auth-fail vlan 500
dot1x critical vlan 500
port-security ntk-mode ntkonly
port-security port-mode userlogin-secure-or-mac
```

2、客户在设备上配置了1X，mac认证和端口安全，下面接的哑终端无法正常经过mac认证注册上线，端口接入模式是userlogin-secure-or-mac，但未配置并行，所以接入的流程是终端1X认证失败，加入到vlan 500，然后等待一段时间mac认证成功，认证成功后会下发vlan 150，加入到vlan 150的网段。发现接入设备上，该mac属于vlan 150，但是在网关设备，该mac地址存在两条表项，分别是vlan 150和vlan 500，终端拿到的mac地址属于vlan 500，arp表项中该mac在vlan 500中。

在5130上面看终端应该是认证成功并获得授权VLAN150了

```
1413-468b-f6e6   150        AUTH            GE2/0/33              N
```

但是上面的网关设备看，MAC在VLAN150和500都存在，终端也是拿到了VLAN500的地址。

```
1413-468b-f6e6   150        Learned         BAGG40                Y
1413-468b-f6e6   500        Learned         BAGG40                Y

10.2.63.156     1413-468b-f6e6 500      BAGG40                8     D
```

过程分析

1、终端发起认证，先加入了guest vlan500，并在vlan500获取了地址

*Dec 3 11:54:35:155 2021 K_D2_Acc_S5130_03-S2 DOT1X/7/EVENT: -Slot=2; Notified Port Sec of new MAC processing result 1: UserMAC=1413-468b-f6e6, VLANID=1, Interface=GigabitEthernet2/0/33.

*Dec 3 11:54:35:156 2021 K_D2_Acc_S5130_03-S2 DOT1X/7/EVENT: -Slot=2; Successfully added a user to guest VLAN 500: UserMAC=1413-468b-f6e6, Interface=GigabitEthernet2/0/33.

2、后面DHCP服务器上也有一条日志，该终端分了一个VLAN 500的ip地址

%Dec 3 11:54:40:566 2021 K_C_Agg_S6520_01 DHCPS/5/DHCPS_ALLOCATE_IP: Server IP = 10.2.62.1, DHCP client IP = 10.2.63.156, DHCP client hardware address = 1413-468b-f6e6, DHCP client lease = 28800 seconds.

3、最后MAC认证成功，S5130将VLAN500去除，终端加入VLAN150，但是终端后面不再去申请新的地址了。对于这种场景，哑终端认证成功后没办法再次去拿地址，就要配置并行，保证其MAC认证先通过。

*Dec 3 11:55:36:291 2021 K_D2_Acc_S5130_03-S2 DOT1X/7/EVENT: -Slot=2; Removed a user from guest VLAN 500: User MAC=1413-468b-f6e6, Interface=GigabitEthernet2/0/33.

*Dec 3 11:55:36:356 2021 K_D2_Acc_S5130_03-S2 PORTSEC/7/EVENT: -Slot=2; MAC [1413-468b-f6e6]: Enable authorization URL: , ifIndex:96, VLANID:150

解决方法

在某些组网环境下，例如用户不希望端口先被加入802.1X的Guest VLAN中，接收到源MAC地址未知的报文后，先触发MAC地址认证，认证成功后端口直接加入MAC地址认证的授权VLAN中，那么需要配置MAC地址认证和802.1X认证并行处理功能和端口延迟加入802.1X Guest VLAN功能。

dot1x guest-vlan-delay new-mac

mac-authentication parallel-with-dot1x