某局点S5560X-54C-EI 设备做MAC认证异常情况排查经验案例

MAC地址认证 端口安全 徐猛 2019-04-04 发表

组网及说明

现场使用我们的S5560X-EI交换机作为接入交换机，一些接口直接连接终端，一些接口连接HUB后，再连接终端，并均在接口上做mac认证。（为保护隐私，本案例中的部分地址信息做了隐匿处理）

问题描述

现场在我们5560X-54C-EI设备上做了mac认证，使用终端直接连接交换机上使能了mac认证的接口的情况下，将终端拔掉后，接到其他使能mac认证的接口上能正常使用。 然后现场将设备40口下接了HUB，然后再接终端，将终端挪到新接口直连上就无法正常使用。

终端接设备上原接口为1/0/40（该接口下联HUB，终端通过HUB连接到交换机40口），新接口为1/0/38。终端MAC地址为f898-b9f1-1994。

1、交换机配置，已经将终端下线检测定时器调整至该参数最小值60，故障依旧：

```
#
 mac-authentication
 mac-authentication timer offline-detect 60
 mac-authentication timer quiet 3600
 mac-authentication domain cinda
#
```

2、查看mac地址表，原接口下已不存在该终端，但是该终端的mac认证表项还是在该接口下

```
#
interface GigabitEthernet1/0/40
 port link-mode bridge
 description V43-Printer-906
 port access vlan 261
 stp edged-port
 poe enable
 mac-authentication
 mac-authentication domain cinda
#
return
[XXXXXXX-vlan261-GigabitEthernet1/0/40]dis mac-add
[XXXXXXX-vlan261-GigabitEthernet1/0/40]dis mac-address  in
[XXXXXXX-vlan261-GigabitEthernet1/0/40]dis mac-address  interface  g
[XXXXXXX-vlan261-GigabitEthernet1/0/40]dis mac-address  interface  GigabitEthernet  1/0/40
MAC Address       VLAN ID    State           Port/Nickname           Aging
f898-b9f0-bded    261        AUTH            GE1/0/40                N
f898-b9f1-20e4    261        AUTH            GE1/0/40                N
f898-b9f1-4f5a    261        AUTH            GE1/0/40                N
[XXXXXXX-vlan261-GigabitEthernet1/0/40]
```

查看接口的mac认证表项：

[XXXXXXX]dis mac-authentication connection interface GigabitEthernet 1/0/40

Slot ID: 1

User MAC address: f898-b9f1-1994

Access interface: GigabitEthernet1/0/40

Username: f898b9f11994

User access state: Successful

Authentication domain: cinda

IPv4 address: *.32.51.32

Initial VLAN: 261

Authorization untagged VLAN: 261

Authorization tagged VLAN: N/A

Authorization VSI: N/A

Authorization ACL ID: N/A

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: N/A

Termination action: Default

Session timeout period: 86400 s

Online from: 2019/02/26 17:11:27

Online duration: 742h 47m 46s

3、跟现场确认新接口关闭mac认证的情况下，可以学习到mac地址，目前业务正常，但是接口未关闭mac认证的情况，新接口学习不到mac地址，终端无法获取IP。

```
#
interface GigabitEthernet1/0/38
 port link-mode bridge
 description V42-905
 port access vlan 261
 stp edged-port
 poe enable
 mac-authentication domain cinda
#
return
[                                -GigabitEthernet1/0/40]dis mac-ad
[                                -GigabitEthernet1/0/40]dis mac-address  in
[                                -GigabitEthernet1/0/40]dis mac-address  interface  g
[                                -GigabitEthernet1/0/40]dis mac-address  interface  GigabitEthernet  1/0/38
MAC Address       VLAN ID    State           Port/Nickname           Aging
f898-b9f1-1994    261        Learned         GE1/0/38                Y
[                                GigabitEthernet1/0/40]
```

过程分析

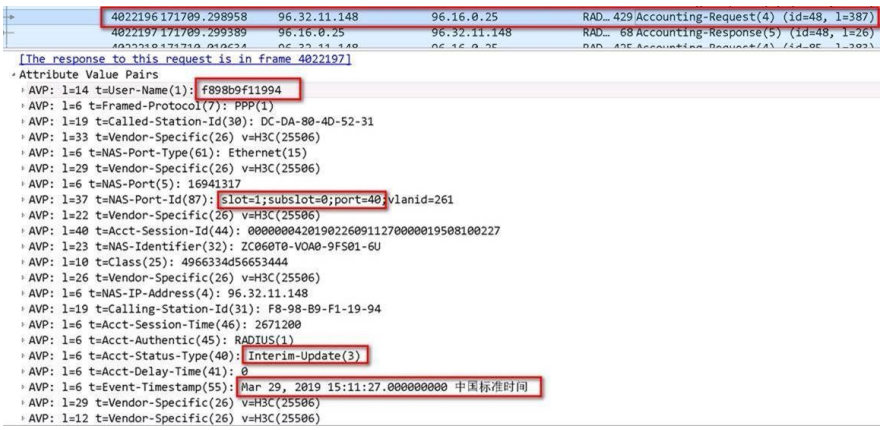
后续现场将终端接入新接口后，收集了一份debug radius信息，其中：

设备地址：#interface Vlan-interface175：ip address *.32.11.148 255.255.255.128
IMC地址：*.16.0.25

终端接到新接口下的Debug记录信息如下，该debug记录为radius的计费更新信息：
debugging radius all *Mar 29 15:23:27:344 2019 XXXXXX MACA/7/EVENT: Sent an accounting-update request: **UserMAC=f898-b9f1-1994,** VLANID=261**, Interface=GigabitEthernet1/0/40.**
*Mar 29 15:23:27:344 2019 XXXXXX MACA/7/EVENT: AAA processed accounting-update request: Result= Processing, **UserMAC=f898-b9f1-1994,** VLANID=261, **Interface=GigabitEthernet1/0/40.**
终端接入在38口并且mac地址学习到38口的情况下，设备还是会发产生该debug计费更新信息，即计费更新的报文，跟现场确认38口无论是否关闭mac认证，设备都会发送终端接在40口下的计费更新报文。

下面为38接口使能mac认证时的设备抓包：

以下为38口关闭mac认证后的抓包情况：



解决方法

进行定位发现：
（1）接口使能mac认证后，终端直接连接的情况下，将终端拔掉后，接口会down，mac表项不会清空，但是认证表项会被清空，所以终端连接到其他接口后，可以重新认证上线。
（2）但是接口连接HUB，在通过HUB连接终端的情况下，终端拔掉后，交换机接口不会down，mac表项不会清空，认证表项不会清空，所以无论终端怎么接，设备都会发送计费更新报文。从而导致终

端无法在新接口上线。
该情况下，需要在设备上：
开启允许MAC迁移功能。
system-view
[Sysname] port-security mac-move permit
说明：缺省情况下允许MAC迁移功能处于关闭状态。MAC迁移功能处于关闭状态时，如果用户从某一端口上线成功，则该用户在未从当前端口下线的情况下无法在设备的其它端口上（无论该端口是否与当前端口属于同一VLAN）发起认证，也无法上线。
MAC迁移功能处于开启状态时，如果用户从某一端口上线成功，则允许该在线用户在设备的其它端口上（无论该端口是否与当前端口属于同一VLAN）发起认证。如果该用户在后接入的端口上认证成功，则当前端口会将该用户立即进行下线处理，保证该用户仅在一个端口上处于上线状态。如果服务器在线用户数已达到上限，将无法进行MAC地址迁移。