

某局点3100V2 dot1x认证失败问题经验案例

一、 组网:

无

二、 问题描述:

客户处有多台S3100V2-8TP-EI设备做接入交换机，起dot1x认证，经常出现用户认证上线时报dot1x连接超时，客户每次以undo dot1x，重启1x解决。

三、 过程分析:

收集诊断信息，发现认证异常时，CPU利用率可以达到100%，其中1x进程比较高。

TaskName	CPU	Runtime(CPU Tick High/CPU Tick Low)
VTYD	0%	0/ 22882c
ND	0%	0/ 34d135
DT1X	83%	0/878bdfbf
ACM	1%	0/ 1b1404e

建议客户在问题复现时，开启debug dot1x all与debug radius packet。3月28日到客户现场分析收集的信息，发现主要原因为认证过程中添加MAC地址表出现问题，而造成规则反复重新下发，进而导致cpu高，具体如下

*Mar 26 14:29:29:481 2014 3100-77 8021X/7/ERROR: The packet will be dropped for the queue is full. -----) 未知mac队列满;

*Mar 26 14:29:29:483 2014 3100-77 8021X/7/EVENT: Succeeded to set EAD rule.

*Mar 26 14:29:29:484 2014 3100-77 8021X/7/EVENT: Succeeded to set EAD HTTP redirection rule.

*Mar 26 14:29:29:486 2014 3100-77 8021X/7/EVENT: Succeeded to set EAD rule.

*Mar 26 14:29:29:487 2014 3100-77 8021X/7/EVENT: Succeeded to set EAD deny rule.

*Mar 26 14:29:29:488 2014 3100-77 8021X/7/ERROR: Failed to add MAC address. -----) 添加mac地址表失败，会删除之前下发的acl规则；这个是导致cpu高的主要原因;

*Mar 26 14:29:29:490 2014 3100-77 8021X/7/ERROR: Failed to add MAC address.

*Mar 26 14:29:29:491 2014 3100-77 8021X/7/EVENT: Succeeded to set EAD rule.

同时，在之前的诊断信息中，发现认证时有mac地址hash冲突的记录，因而怀疑很可能为mac地址hash冲突，导致mac地址添加失败。

```

=====
=====debug l2 1 0 mac/hashconflict/show=====
=====
mac      vlanid  modid  port  bucket
1 00:44:e6:09:11:df, 104, 0, 5, 0

```

四、 解决方法:

明确了问题的原因之后，查看用户配置，发现客户S31V2设备上行口g1/0/9原来 permit vlan all，有学到很多多余mac。

先指导客户裁剪vlan，改为只允许必要vlan通过后，mac表项由原来1700以上减为200以下，通过减少mac地址的透传来大大减少mac地址hash冲突的发生。

修改配置之后继续观察，问题不再复现。

