某局点 dot1X 多次认证才能上线且21分钟下线 案例

802.1X 张华野 2020-02-27 发表

组网及说明

S10500 做dot1X认证

问题描述

故障现象：

客户处用S10500进行dot1X认证，发现客户多次认证才能上线，认证次数无规律。上线之后21分钟准时掉线，而且认证成功之后终端点击下线之后仍然在线。

过程分析

故障分析：

1）由于dot1X认证需要占用acl资源，设备资源不足导致 dot1X acl没有下发到硬件。

%Oct 11 16:44:23:169 2019 HJ-Dzuo-H3C-S10506-00 DOT1X/3/DOT1X_NOTENOUGH_ENABLEDOT1X_RES: -Chassis=1-Slot=4; Failed to enable 802.1X on interface Bridge-Aggregation38 due to lack of ACL resources.

查看硬件资源，包过滤占用了大量的acl资源：

```
====debug qacl show acl-resc chassis 1 slot 4 chip 0====
  acl type                usedEntries[2197]
 ========================================
  [100]PktFilter IP on VRF       47
  [215]PktFilter IP on L3 VSI      2150
 ========================================
Acl Hw Resource: IFP, Pipe 0
 ====================================
             entrynum  counternum  meternum
 total       : 16384    8192       8192
 total-reserved : 6144     3072       3072
 used-reserved  : 334      162        121
 used-useracl   : 4499     0          0
 free-useracl   : 5741     5120       5120
 ====================================
```

2）优化acl资源之后，聚合口下dot1X acl没有继续向硬件下发。如果dot1X下发在物理口，设备检测到acl资源不足会命令行回退，如果下发在聚合口，存在聚合口的成员口分布在不同单板的场景，此时保障实现功能优先，不会检测acl资源后回退命令。所以acl资源优化之后没有立即恢复。

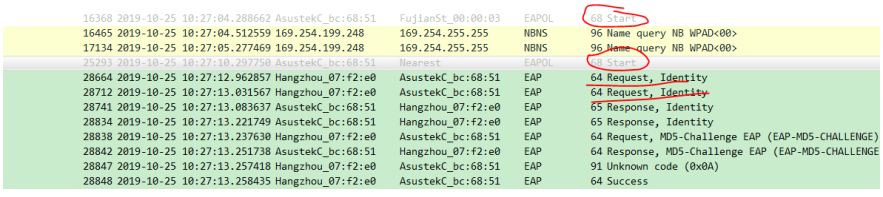
3）Dot1X认证存在卡顿原因分析：

Dot1X认证由终端发起的EAPOL start报文触发，在正常情况下，设备acl资源充足时，会下发acl到硬件，此时按照dot1X类型报文上送cpu进行处理。如果底层没有下发dot1x类型acl，现场的报文匹配了L2MISS_SMAC类型上送cpu处理，L2MISS_SMAC与new mac事件上报队列一起上送。但是由于该队列报文较多（设备debug信息也一直在上报new mac事件），导致夹杂在其中的dot1x start报文处理较慢（有时甚至会被丢弃），从而表现为卡顿。现网现象也表现为有时会卡顿几次，但有时也能够一次上线。

```
====debug rxtx softcar show chassis 1 slot 4====
ID  Type              RcvPps Rcv_All    DisPkt_All Pps  Dyn Swi Hash ACLmax
38  DOT1X               20    1134314    0          300  S   On  SMAC 8
157 L2MISS_SMAC         6     1473494    3743       100  S   On  SMAC 0
```

终端依次发了两个dot1x start报文，设备过了一段时间才回复request报文。

抓包如下：



4）21分钟掉线原因分析：

在终端成功上线后，由于已经学习到了终端的mac地址，后续的dot1x心跳报文和下线报文就不会再命中softcar 中“L2MISS_SMAC”类型报文上送cpu。所以表现为客户端点击下线不生效，以及心跳报文接收不到。

21分钟后掉线原因为：心跳报文发送周期为3分钟，重试6次，再加上开始3分钟，所以一共为21分钟。

解决方法

优化ACL：

删除不用的ACL

合并类似的ACL