某局点收到大量组播导致802.1X掉线问题

802.1X IGMP 李鹏飞 2022-01-25 发表

组网及说明

不涉及

问题描述

2框5槽位单板下连dot1x认证终端出现异常下线，影响到终端的外部访问；现网为排除单板硬件故障，将2框5槽位单板下的业务迁移到2框2槽位，20号2框2槽位下连的dot1x认证终端再次出现异常下线

过程分析

1、认证服务器侧分析终端下线原因是：2（Lost Carrier），即：设备开启dot1x在线用户握手功能后，设备会定期（默认15s）向在线的dot1x用户发送握手请求报文，以定期检测用户的在线情况，如果设备连续多次（默认3次）没有收到客户端的应答报文，则会将用户置为下线状态。分析设备诊断日志，故障时间点前后都记录了一些内部转发路径报错的信息，进一步分析发现1框、2框的多块单板都会出现上述现象，怀疑是单板cpu处理的报文过多，导致像内部检测报文、dot1x报文等，无法及时处理：

%@26173^Jan 19 14:03:48:038 2021 QHJR_BG_21FHX01_10508 DRVPLAT/3/DrvDebug: -Chassis=2-Slot=5; LINE:2542 MOD:MAC,TASK:DFWK,-FILE id 0x40,SLOT:28--: Forward check fail! p1=128; (23.0.18)->(33.0)->(28.0)

2、进一步搜集信息，发现设备出现内部转发路径报错时，对应单板都会出现bRX1进程收包任务的cpu占用率短暂升高现象：

1126 14.2% 0.5% 0.4% [bRX1]

3、查询发现CPU占用升高时，单板5s内突然会发送大量报文，而正常时只有几百个左右；进一步尝试将报文打印出来解析，发现都是239.255.255.250的组播报文，这个组播地址是Windows系统SSDP协议使用的，是windows系统自带的服务，默认打开，设备启动后会定时发送该组播地址的报文

```
RxDv: Dv=8,Dvhead=0xffff800026641228,Dvtail=0xffff800026641628,token=12000,Pps=12000
TxDv: Dv=0,Dvactive=0x        (null),Dvfree=0xffff800042bfe028,Dvfreecnt=32
Intr: Desc=426,Chain=13645,Tx=13530,Rx=922,Chain_err=0,Chain_recover=0,Max_Intrmask=0
Task: Plat=327,VlanTx=5,TxOk=13530

*Jan 25 16:27:59:706 2021 QHJR_BG_21FHX01_10508 DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=1-Slot=5;
 drv_rxtx_tx_intfphytransmit():ulIfIndex=0x200,priority=3,length=173,MbufFlag=0x4800002,task:bRX1
*Jan 25 16:27:59:706 2021 QHJR_BG_21FHX01_10508 DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=1-Slot=5;
 drv_rxtx_tx_porttransmit():mod=10,port=3,priority=3,length=173
*Jan 25 16:27:59:706 2021 QHJR_BG_21FHX01_10508 DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=1-Slot=5;
 drv_rxtx_tx_rawtransmit():unit=0,port=3,priority=3,length=173
*Jan 25 16:27:59:706 2021 QHJR_BG_21FHX01_10508 DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=1-Slot=5;
From board 5: transmit packet from chip0,port3,Priority=3,len=173
-----------------------------------------------------
0000  01 00 5e 7f ff fa 00 00 00 00 00 01 81 00 00 7c
0010  08 00 45 00 00 9b a9 0d 00 00 03 11 06 b5 09 03
0020  0e 93 ef ff ff fa d6 0f 07 6c 00 87 e2 5f 4d 2d
0030  53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e
0040  31 0d 0a 48 6f 73 74 3a 20 32 33 39 2e 32 35 35
0050  2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d 0a 53
0060  54 3a 20 75 75 69 64 3a 34 65 35 65 34 62 65 32
0070  2d 65 30 62 32 2d 61 65 63 66 2d 31 61 30 62 2d
0080  30 32 63 63 36 34 61 65 30 62 33 37 0d 0a 4d 61
0090  6e 3a 20 22 73 73 64 70 3a 64 69 73 63 6f 76 65
00a0  72 22 0d 0a 4d 58 3a 20 33 0d 0a 0d 0a
-----------------------------------------------------
```

4、现网所有vsi接口都开启了三层组播、配置了组加入，所有windows终端默认都会定时发送239.255.255.250的组加入及数据报文，对于设备相当于每个终端即是组播源又是组播接收者。设备在硬件组播表项生成前这些报文属于未知组播，收到这种报文后会上送单板cpu触发组播表项学习，根据协议要求，cpu在学习组播表项的同时还会对报文进行软转，在某一时刻windows终端并发SSDP协议组播报文，组播报文数量和接口数量的增加会导致发包耗时陡增，以至于影响到dot1x以及其他报文的处理；而在下发硬件表项之后，对应组播流直接走硬件转发，不会再上送cpu处理，dot1x以及其他报文的处理不再收到影响。

解决方法

由于现网不会使用239.255.255.250这个组播组，增加配置对该地址进行了过滤，配置后观察设备运行平稳，没有再出现之前的异常现象。

下发在PIM协议上的规则，禁止239.255.255.250生成(S,G)表项。

```
acl number 3000
  rule 0 deny ip destination 239.255.255.250 0
  rule 5 permit ip
pim
  register-policy 3000
  source-policy 3000
```