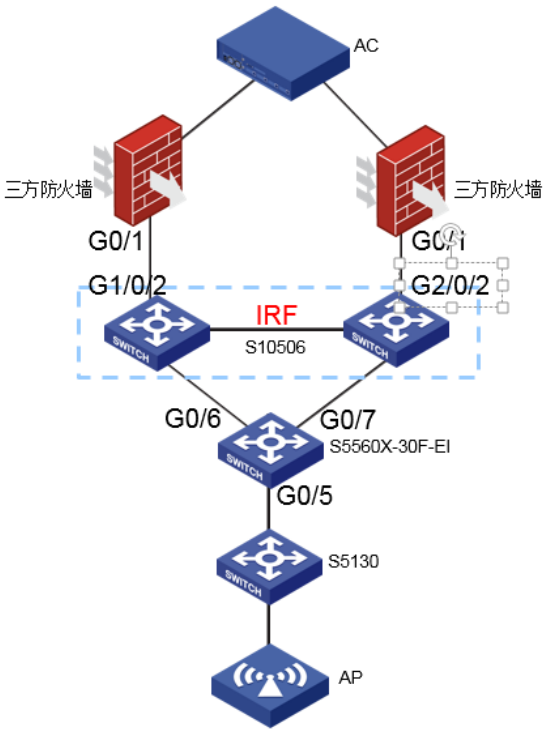
某局点AP过S5560X-30F-EI交换机无法注册到AC故障排查经验案例

二层链路聚合　王周华　2019-11-30 发表

组网及说明

现场AC下挂两台三方防火墙，两台三方防火墙设备独立运行，通过G0/1口连接到我司的S10506设备。两台S10506设备之间配置了IRF，通过等价路由将数据包转发给三方防火墙，S10506两个成员设备各出一根线和下连的单台5560X-30F-EI通过聚合口互联。5560X-30F-EI上的聚合口的成员接口是6口和7口，通过5口连接到poe交换机S5130，S5130为AP供电。组网大致拓扑图如下：



本次涉及设备的型号以及版本： S5560X-30F-EI　Version 7.1.070, Release 1110

问题描述

现场工程师反馈三方产商的AP设备无法注册到AC上，怀疑AP和AC之间交互的报文被丢弃了，导致了该问题。

过程分析

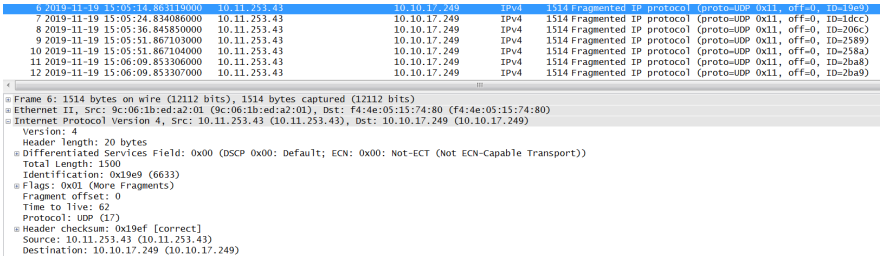
1、首先需保证流量经过我们设备时不会被丢弃和走了其它的转发路径，和现场工程师确认我们的交换机上没有配置包过滤和策略路由，其它流量过设备转发正常，说明应该不会是链路问题导致。

2、接下来需要排查三方产商的防火墙是否将流量丢弃了。于是让现场工程师在防火墙的接口抓包确认流量是否有上送到防火墙设备，现场工程师在两台防火墙连接交换机和连接AC的接口抓包。发现在两台防火墙连接交换机的接口均抓到了AP发往AC的交互报文，但是在连接AC的接口抓包发现只有左侧的防火墙将报文转发了出去。

左侧防火墙抓包：

```
    28 2019-11-19 15:05:13.750768000   10.11.253.43                10.10.17.249        IPv4      125 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=19e9)
    29 2019-11-19 15:05:23.751724000   10.11.253.43                10.10.17.249        IPv4      125 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=1dcc)
    30 2019-11-19 15:05:35.750997000   10.11.253.43                10.10.17.249        IPv4      125 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=206c)
    31 2019-11-19 15:05:50.750870000   10.11.253.43                10.10.17.249        IPv4      125 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=2589)
    32 2019-11-19 15:05:50.750870000   10.11.253.43                10.10.17.249        IPv4       93 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=258a)
    33 2019-11-19 15:06:08.750988000   10.11.253.43                10.10.17.249        IPv4      125 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=2ba8)
    34 2019-11-19 15:06:08.751013000   10.11.253.43                10.10.17.249        IPv4       93 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=2ba9)
    35 2019-11-19 15:06:31.751166000   10.11.253.43                10.10.17.249        IPv4      125 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=308d)
    36 2019-11-19 15:06:31.751186000   10.11.253.43                10.10.17.249        IPv4       93 Fragmented IP protocol (proto=UDP 0x11, off=1480, ID=308e)
⊞ Frame 28: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits)
⊞ Ethernet II, Src: 9c:06:1b:ed:a2:01 (9c:06:1b:ed:a2:01), Dst: f4:4e:05:15:74:80 (f4:4e:05:15:74:80)
⊟ Internet Protocol Version 4, Src: 10.11.253.43 (10.11.253.43), Dst: 10.10.17.249 (10.10.17.249)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 111
    Identification: 0x19e9 (6633)
  ⊞ Flags: 0x00
    Fragment offset: 1480
    Time to live: 62
    Protocol: UDP (17)
  ⊞ Header checksum: 0x3ea3 [correct]
    Source: 10.11.253.43 (10.11.253.43)
    Destination: 10.10.17.249 (10.10.17.249)
```

右侧防火墙抓包：

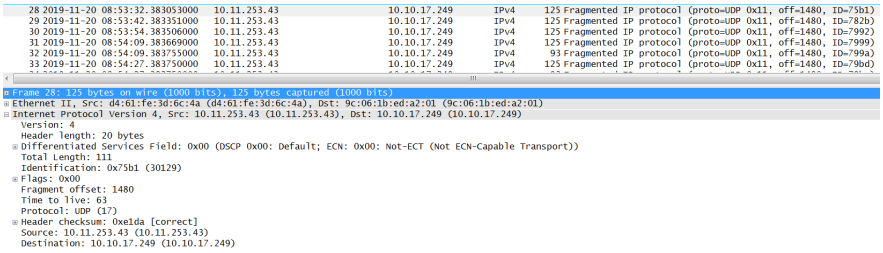


于是确定了是部分流量经过右侧防火墙后被丢弃导致的该问题。现场工程师进一步确认防火墙丢弃报文的原因是同一五元组数据流先是在左侧防火墙上创建了会话信息，但是后续上来的报文又发送到了右侧防火墙，右侧防火墙上没有相应的会话信息，导致了流量被丢弃。

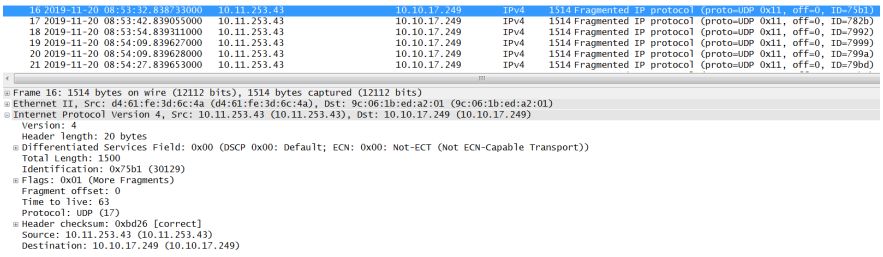
3、结合现场情况我们进一步排查同一五元组的数据流但是走了不同的转发路径的原因。现场两台S10506上配置了等价路由的方式将报文转发给防火墙，确认该版本等价路由默认情况下是按照五元组加上入接口逐流转发，且两台S10506配置了IRF，对于IRF的设备遵循本框转发优先的原则，于是怀疑上送到S10506设备的报文本身就是从两个不同的成员设备接口上来的。

4、因此让现场工程师在S5560X-30F-EI设备连接S10506设备的聚合口的两个成员接口G0/6和G0/7接口以及下连S5130接口G0/5抓包,发现从G0/5接口上来的报文分别从G0/6接口和G0/7口接口转发。

G0/6口抓包：



G0/7口抓包：



于是确认流量是在S5560X-30F-EI上分流了，S5560X-30F-EI和S10506之间是通过聚合口连接的，现场的S5560X-30F-EI版本是Version 7.1.070, Release 1110，该版本聚合口负载分担的类型是按照报文类型选择，老的版本Hash时使用了过长的Hash掩码，导致了使用了源目的Ip及 源目的Mac之外的Hash 因子，使得Hash后的同一五元组数据流走了不同的成员接口。

解决方法

1、升级版本至最新版本，最新版本聚合口缺省情况下采用了逐流转发的负载分担方式，使属于同一数据流的报文从同一条成员链路上通过。

2、配置基于目的ip和源ip组合的方式逐流负载分担link-aggregation load-sharing mode source-ip destination-ip。