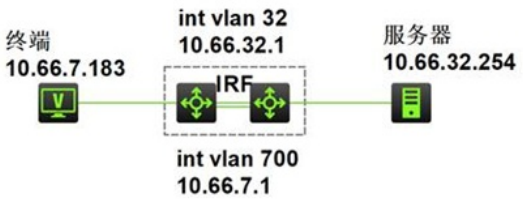
某局点S7506E-X 交换机特定网段三层转发间歇性不通问题

IP转发 ARP攻击防御 苏亚东 2021-08-05 发表

组网及说明

某局点用两台S7506E-X作为网关设备，交换机SW1和SW2之间做了堆叠。现场终端通过S7506E-X访问vlan 32内的其他服务器存在间歇性不通的情况。



问题描述

从终端ping 目的地址10.66.32.254的服务器测试，流统可以看到报文丢在了交换机上。vlan 32内业务二层互访无问题，跨三层访问会有不通、丢包等问题；即10.66.7.183 ping 10.66.32.254会间歇性不通，10.66.32.0/24同网段二层转发正常，10.66.7.0/24网段二三层转发均正常

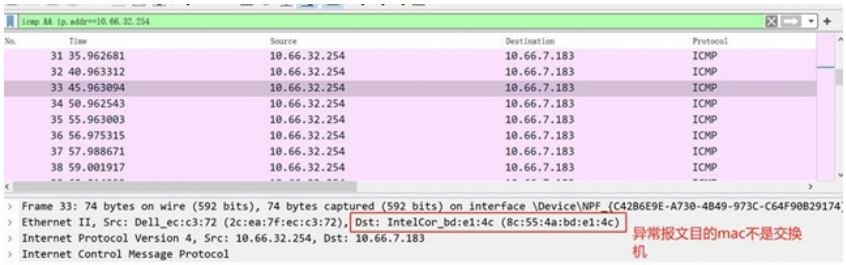
过程分析

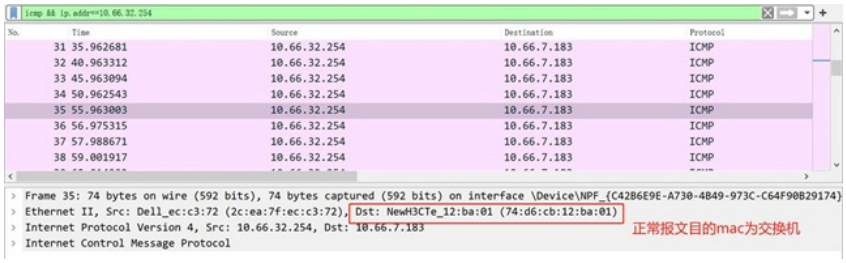
1、 根据反馈的诊断查看设备相关信息，设备上无硬件相关报错，端口无CRC、设备未开启生成树，通过梳理组网现场流量为跨框跨板卡流量，初步怀疑是个别板卡之间表项同步或者通信存在异常；

2、 远程到设备上查看信息，发现各个板卡上arp表项均正常，查看板卡之间互连hg口、堆叠口也都无错包、拥塞等情况，调整PC到交换机同板卡同芯片时故障依旧，根据这些信息基本可以排除交换机侧的硬件问题；

```
 ====display devm hgport chassis 2 slot 0====
 (chassis 2 slot 0, chassis 2 slot 6):

(unit, port)  (unit port)
(0  , 52 )  (0  , 3  )
(chassis 2 slot 0, chassis 2 slot 7):

(unit, port)  (unit port)
(0  , 51 )  (0  , 3  )

     hg4( 51)  up    42G  FD   SW  No   Forward       None   FA   KR4  9416

     hg5( 52)  up    42G  FD   SW  No   Forward       None   FA   KR4  9416

 ====display devm hgport chassis 2 slot 3====
(chassis 2 slot 3, chassis 2 slot 0):

Error PortNum=0
(chassis 2 slot 3, chassis 2 slot 6):

(unit, port)  (unit port)
(0  , 54 )  (0  , 14 )
(chassis 2 slot 3, chassis 2 slot 7):

(unit, port)  (unit port)
(0  , 55 )  (0  , 14 )

     hg1( 54)  up    42G  FD   SW  No   Forward       None   FA  XGMII 16360

     hg2( 55)  up    42G  FD   SW  No   Forward       None   FA  XGMII 16360
```

4、 通过流统发现不通时访问的回程报文到达交换机后未继续转发回终端，产生丢包。通过镜像抓包确认，丢包时服务器10.66.32.254回复报文的目的mac（8c55-4abd-e14c）并不是交换机上的接口地址（74d6-cb12-ba01），对于交换机而言，只有目的mac是自己的报文才会解封装进行三层转发，而现场造成丢包的报文的目的mac是接在核心xge1/0/0/11口下的一个终端的mac，导致交换机进行二层转发；





Vlan-interface32

Current state: UP

Line protocol state: UP

Internet address: 10.66.32.1/24 (Primary)

IPv4 packet frame type: Ethernet II, hardware address: 74d6-cb12-ba01

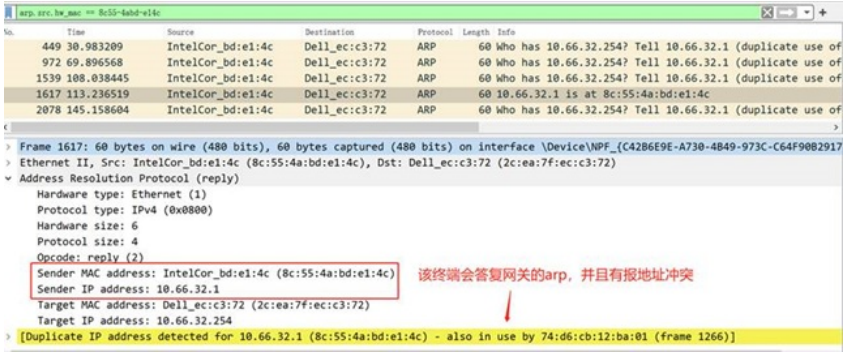
IPv6 packet frame type: Ethernet II, hardware address: 74d6-cb12-ba01

2、在核心XGE1/0/0/11下的接入交换机上对应接口下配置了arp网关保护arp filter source，现场采用这种方式配置后故障恢复。

==========display mac-address==========

MAC Address	VLAN ID	State	Port/Nickname	Aging
8c55-4abd-e14c	32	Learned	XGE1/0/0/11	Y

5、 此时已经可以确认非交换机问题。经排查，8c55-4abd-e14c这个mac应该是现场某个终端小车的mac地址，通过无线连接在核心XGE1/0/0/11接口下的接入交换机上。为了定位问题继续抓包查看服务器互连端口进出的报文，发现该mac地址会给服务器答复网关的arp，因此导致服务器arp学习错误、报文封装异常，因此三层转发出现间歇性丢包。而二层转发并不需要经过网关，所以没有问题。



6、 综合以上，判断现场的小车可能是误配置了网关的ip地址，存在地址冲突的情况，导致该vlan内其他端口下的设备arp学习异常；另外，小车只是会回复其他终端请求网关的arp，并不会因为地址冲突发免费arp，所以交换机侧无法感知到。

解决方法

针对这种情况，可以通过以下两种途径来解决问题：

1、排查对应终端是否存在地址配置错误的情况，如有则更改；

2、在核心下的接入交换机上配置arp filter source。