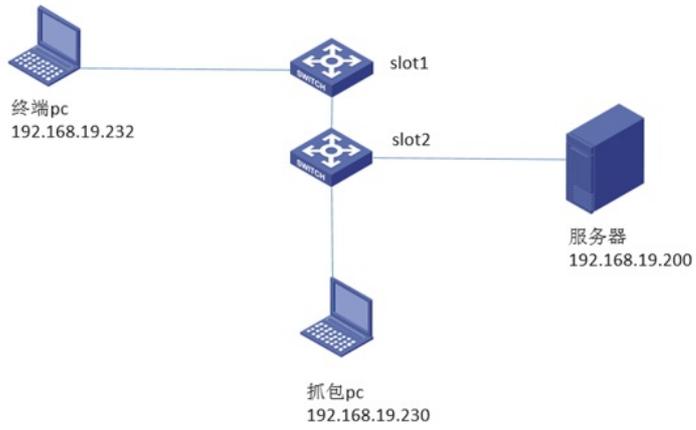


知 S5130S-EI交换机能抓到其他接口单播流量

MAC地址表 STP IRF2 孙兆强 2021-04-30 发表

组网及说明



两台S5130S-EI交换机做了IRF2，终端pc接在slot1上，抓包pc接在slot2上。PC和服务器同网段。

问题描述

终端pc和服务器同网段，pc访问服务器业务正常，业务为tcp流量。抓包pc只要接到slot2上开启抓包就能抓到终端pc的单播流量。在设备上查看接口mac地址学习正常

No.	Time	Source	Destination	Protocol	Length	Info
729	2021-03-11 20:12:55.895298	192.168.19.200	192.168.19.232	TCP	1062	655 → 65464 [PSH, ACK] Seq=6961 Ack=1 Win=32757 Len=1008
730	2021-03-11 20:12:55.899804	192.168.19.200	192.168.19.232	TCP	60	655 → 65447 [PSH, ACK] Seq=3085 Ack=1 Win=32747 Len=4
731	2021-03-11 20:12:55.899804	192.168.19.200	192.168.19.232	TCP	390	655 → 65447 [PSH, ACK] Seq=3089 Ack=1 Win=32747 Len=336
732	2021-03-11 20:12:55.904971	192.168.19.200	192.168.19.232	TCP	60	655 → 65464 [PSH, ACK] Seq=7969 Ack=1 Win=32757 Len=4
733	2021-03-11 20:12:55.920511	192.168.19.200	192.168.19.232	TCP	1514	655 → 65447 [ACK] Seq=3425 Ack=1 Win=32747 Len=1460
734	2021-03-11 20:12:55.920511	192.168.19.200	192.168.19.232	TCP	1514	655 → 65447 [ACK] Seq=4885 Ack=1 Win=32747 Len=1460
735	2021-03-11 20:12:55.920511	192.168.19.200	192.168.19.232	TCP	1022	655 → 65447 [PSH, ACK] Seq=6345 Ack=1 Win=32747 Len=968
736	2021-03-11 20:12:55.933468	192.168.19.200	192.168.19.232	TCP	60	655 → 65435 [PSH, ACK] Seq=1 Ack=1 Win=32747 Len=4
737	2021-03-11 20:12:55.933468	192.168.19.200	192.168.19.232	TCP	1514	655 → 65435 [ACK] Seq=5 Ack=1 Win=32747 Len=1460
738	2021-03-11 20:12:55.933468	192.168.19.200	192.168.19.232	TCP	1514	655 → 65435 [ACK] Seq=1465 Ack=1 Win=32747 Len=1460
739	2021-03-11 20:12:55.933468	192.168.19.200	192.168.19.232	TCP	582	655 → 65435 [PSH, ACK] Seq=2925 Ack=1 Win=32747 Len=528
740	2021-03-11 20:12:55.936415	192.168.19.200	192.168.19.232	TCP	1514	655 → 65464 [ACK] Seq=7973 Ack=1 Win=32757 Len=1460
741	2021-03-11 20:12:55.936415	192.168.19.200	192.168.19.232	TCP	1514	655 → 65464 [ACK] Seq=9433 Ack=1 Win=32757 Len=1460
742	2021-03-11 20:12:55.936415	192.168.19.200	192.168.19.232	TCP	986	655 → 65464 [PSH, ACK] Seq=10893 Ack=1 Win=32757 Len=932

过程分析

在交换机上display mac-address查看终端pc和服务器的mac学习正常。

查看目的地址的交换机底层mac信息

slot2底层无目的mac信息。

```
[CCTV_CORE-probe]debug 12 slot 2 chip 0 mac/find/vid=18/mac=08:94:ef:aa:3c:a1

find mac 08:94:ef:aa:3c:a1 in vlan 18
*****unit 0: *****
unit 0: entry not found
```

slot1底层有目的mac

```
[CCTV_CORE-probe]debug 12 slot 1 chip 0 mac/find/vid=18/mac=08:94:ef:aa:3c:a1

find mac 08:94:ef:aa:3c:a1 in vlan 18
*****unit 0: *****
unit 0: entry found
  uiIndex 8564
  validPtr 1
  skipPtr 0
  agedPtr 1
  mod 2, port 12,
isStatic=0 type=(0x00000000):
daCommand=0
saCommand=0
daRoute=0
mirrorToRxAnalyzerPortEn=0
sourceID=2
daQosIndex=0
saQosIndex=0
daSecurityLevel=0
saSecurityLevel=0
appSpecificCpuCode=0
spUnknown=0
saMirrorToRxAnalyzerPortEn=0
daMirrorToRxAnalyzerPortEn=0
entry detail type 0: DRV_MAC_DYNAMIC_HARDWARE_LEARNED | ;
----- find the mac -----

MAC=08:94:ef:aa:3c:a1,vlan=18,index=8564,mod=2,port=12,LEARNED;
----- find mac end -----
```

流量从服务器到交换机，从lot2转发到slot1。因为slot2的底层没有slot1的mac所以会以广播的形式发送。抓包pc和服务器属于同网段所以能抓到报文。

解决方法

IRF设备通常有多个成员设备，为了避免不必要的广播报文，以及提高报文转发的速度，需要所有成员设备拥有同样的MAC地址表。开启全局的MAC地址同步功能后，设备会在所有成员设备间进行MAC地址表的同步。

```
[system] mac-address mac-roaming enable
```

正常情况下终端pc访问服务器时首先会发arp广播报文，这样slot1和slot2都能学习到终端pc的mac。但是现场没有开启stp 边缘端口，抓包pc接入之后导致stp重新计算，导致接口下mac刷新。又因此时客户端pc和服务器之间交互的是单播报文，从而slot2无法学习到终端pc的mac。所以交换机上需要同时开启边缘端口。

```
[SW-GigabitEthernet1/0/3]stp edged-port
```

或者全局关闭stp（不推荐）

```
[SW]undo stp global enable
```

