某局点S6300特性VLAN 97 不通问题

VLAN 二层转发 许鹏鹏 2020-02-25 发表

组网及说明

思科3945路由器和6300对接，GE_0/1口 access vlan 96，起一个interface vlan96的ip 1.1.1.1 。 6300上GE_0/1口也是access vlan 96，GE_0/2也是access vlan96，GE_0/3是access vlan97，在6300上起interface vlan97的ip 1.1.1.2。防火墙是透明模式，两个接口都是属于vlan 4088。拓扑如图1所示：

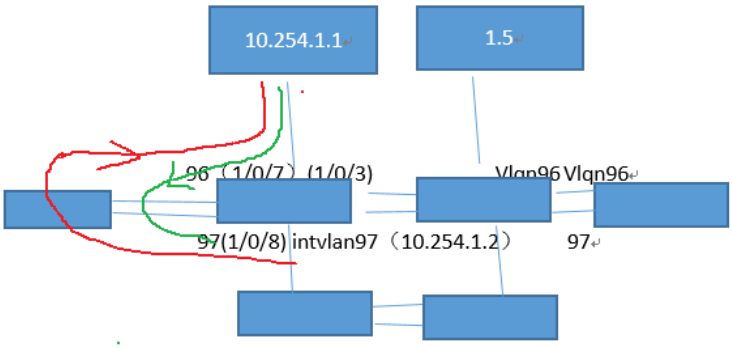

图1

问题描述

通过1.1.1.1 去ping1.1.1.2的时候，流量会按照红色箭头方向走。 现场反馈将端口按以上描述划分在96,97的时候，这样无法ping通

过程分析

查看arp也没学到对端1.1.1.1的arp，设置成800多也无法ping通，将vlan id设置成1000以上，如1000和1001，并起个interface vlan 1001的地址才可以ping通。怀疑可能是防火墙问题，但是后面排查发现防火墙是透明模式，且交换机接口都是access口，出去都会剥离标签，和vlan id应该没关系。
另外客户反馈，将设备上vlan 97地址去除，设置在6300下挂的一台pc上的时候，可以ping通对端1.1.1.1 。

现场复现：
测试是在6300上用10.254.1.2地址去ping路由器上10.254.1.1这个地址的。通过流统可以看到从3口有进，有出报文，从7口只有进的报文，没有出的报文。

```
[CLOUD_ZHUANXIAN_SW_S6300]display qos policy in
[CLOUD_ZHUANXIAN_SW_S6300]display qos policy interface
Interface: Ten-GigabitEthernet1/0/3
  Direction: Inbound
  Policy: 1to2
   Classifier: 1to2
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: 1to2
      Accounting enable:
        5 (Packets)

Interface: Ten-GigabitEthernet1/0/3
  Direction: Outbound
  Policy: 2to1
   Classifier: 2to1
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: 2to1
      Accounting enable:
        5 (Packets)
```

```
Interface: Ten-GigabitEthernet1/0/7
  Direction: Inbound
  Policy: 2to1
   Classifier: 2to1
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: 2to1
      Accounting enable:
        5 (Packets)

Interface: Ten-GigabitEthernet1/0/7
  Direction: Outbound
  Policy: 1to2
   Classifier: 1to2
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: 1to2
      Accounting enable:
        0 (Packets)

Interface: Ten-GigabitEthernet1/0/8
  Direction: Inbound
  Policy: 1to2
   Classifier: 1to2
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: 1to2
      Accounting enable:
        0 (Packets)

Interface: Ten-GigabitEthernet1/0/8
  Direction: Outbound
  Policy: 2to1
   Classifier: 2to1
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: 2to1
      Accounting enable:
        0 (Packets)

Interface: Ten-GigabitEthernet2/0/7
  Direction: Inbound
  Policy: 2to1
   Classifier: 2to1
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: 2to1
      Accounting enable:
        0 (Packets)

Interface: Ten-GigabitEthernet2/0/7
  Direction: Outbound
  Policy: 1to2
   Classifier: 1to2
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: 1to2
```

Accounting enable:
0 (Packets)

Interface: Ten-GigabitEthernet2/0/8
Direction: Inbound
Policy: 1to2
Classifier: 1to2
Operator: AND
Rule(s) :
If-match acl 3000
Behavior: 1to2
Accounting enable:
0 (Packets)

Interface: Ten-GigabitEthernet2/0/8
Direction: Outbound
Policy: 2to1
Classifier: 2to1
Operator: AND
Rule(s) :
If-match acl 3001
Behavior: 2to1
Accounting enable:
0 (Packets)

流量走向说明：ping出去报文红色箭头，回程报文绿色箭头，现在从1/0/7没有出去的报文，怀疑丢在了6300

打印出的报文内容显示，如图2所示，对端发来的报文带的是valn 97 的tag , 同时6300侧一直有rdbgc3（vlan检查失败丢包） 增长。可能是内对端发错包或者报文进端口被打错了标签

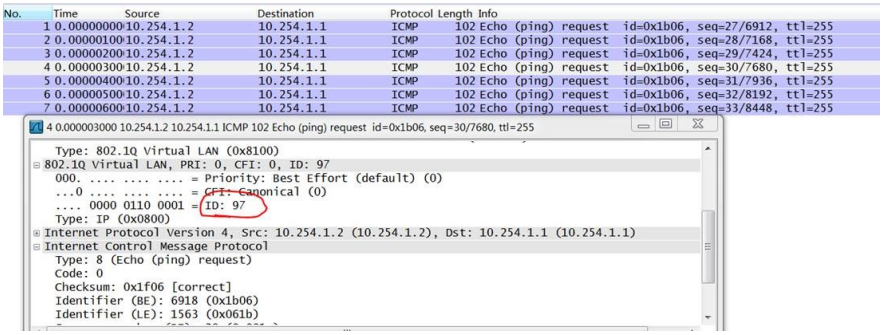

图2

*Jan 16 09:24:35:111 2011 CLOUD_ZHUANXIAN_SW_S6300 DRVPLAT/7/RxTxDebug:
From board 1: transmit packet from chip0,port8,Priority=3,len=102

```
----------------------------------------------------
0000  00 3a 7d fc 5f 01 dc da 80 ee a3 49 81 00 00 61
0010  08 00 45 00 00 54 4f 7b 00 00 ff 01 54 2f 0a fe
0020  01 02 0a fe 01 01 08 00 39 ac 1b 06 00 1c 4d 32
0030  b9 53 00 01 b1 a7 08 09 0a 0b 0c 0d 0e 0f 10 11
0040  12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0050  22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
0060  32 33 34 35 36 37
----------------------------------------------------
```

RDBGC3.xe2 : 3,006 +482 71/s

后面经过实验室复现，发现是版本bug，在支持trill 的版本上， vlan 1 的mac和启动初始化的trill mac 创建的相关三层表项冲突，会匹配上三层转发。我们设备的mac分配是按照32个一轮分配的， 也就是 vlan 为 32*N + 1 的， 和vlan 1 的mac 是相同的。现场97 正好就是。因此会出现客户环境上目的mac 是 vlan interface97的报文匹配上了三层转发而丢包。导致ICMP replay报文没有二层透传到防火墙。因此客户处的现象会是配置interface 97，然后配vlan 96 、300 、1000等都不行， 使用 vlan interface 1000 配合 vlan 1001 是正常的。规律就是 vlan interface 使用 32*n+1 的ID在这种绕行方案的组网下会不通， 规避方法是 在interface vlan 不使用 32*n+1 的id 号。规避方法实验室已初步验证成功。 63 的l3 interface 规格只有32，避开32*n+1，ID号也是足够用的。

解决方法

规避方法是 在interface vlan 不使用 32*n+1 的id 号。最终解决办法是打上R2432P05H10补丁。