因STP配置不当特定情境下终端无法获取IP地址案例分析

STP 孔天娇 2015-01-05 发表

PC MAC：0C:C4:7A:0F:2D:48

客户组网可简化为业务终端、S5120HI二层交换机、DHCP　Server三个部分。其接口连接关系如上图：S5120HI 1/0/13口下连终端、1/0/14口上联DHCP Server。其中业务终端分为已安装系统的终端和未安装系统的终端，未安装系统的client需要从DHCP Server得到地址之后去应用服务器下载系统

据客户反馈当前连接到一台S5120HI设备上未安装系统的client无法获取地址。client和server用网线直连可以获得地址，更换其他S5120HI可以得到地址。但该S5120HI下其他有系统的终端能够正常获取到IP地址。客户通过做镜像抓包发现：在S5120HI连接DHCP Server的接口1/0/14未发送DHCP DISCOVER报文。由此客户怀疑是S5120HI转发有问题，将DHCP报文丢弃。

此处S5120HI作为纯二层设备，基本的二层广播报文泛洪不应有问题。且客户描述获取不到地址的情况还有终端类型（是否安装系统相关），交换机是不会也无法做这些区分的。怀疑还是跟现场环境相关。

1、同时在S5120HI上下行口做镜像和流统计，确认包是否丢在S5120HI上。

关键配置如下：

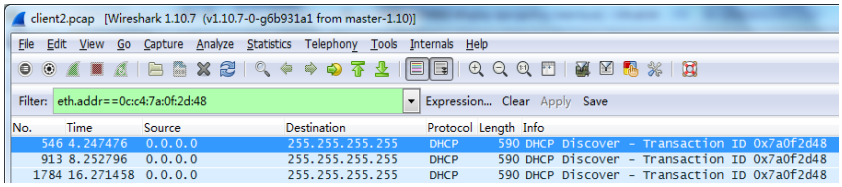
```
mirroring-group 1 local
mirroring-group 2 local

interface GigabitEthernet1/0/13
   port access vlan 105
   qos apply policy 1 inbound
   mirroring-group 1 mirroring-port inbound

interface GigabitEthernet1/0/14
 port access vlan 105
qos apply policy 1 outbound
mirroring-group 1 mirroring-port outbound

interface GigabitEthernet2/0/14
 mirroring-group 1 monitor-port
interface GigabitEthernet2/0/16
 mirroring-group 2 monitor-port

acl number 4000
 rule 0 permit source-mac 0cc4-7a0f-2d48 ffff-ffff-ffff
traffic classifier 1 operator and
 if-match acl 4000
traffic behavior 1
 accounting packet
qos policy 1
 classifier 1 behavior 1
```

流统计信息如下：

```
display  qos policy interface
  Interface: GigabitEthernet1/0/13
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 4000
     Behavior: 1
      Accounting Enable:
        193 (Packets)

  Interface: GigabitEthernet1/0/14
  Direction: Outbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 4000
     Behavior: 1
      Accounting Enable:
        0 (Packets)

display  qos policy interface
  Interface: GigabitEthernet1/0/13

  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 4000
     Behavior: 1
      Accounting Enable:
        207 (Packets)
```

Interface: GigabitEthernet1/0/14
Direction: Outbound
Policy: 1
Classifier: 1
Operator: AND
Rule(s) : If-match acl 4000
Behavior: 1
Accounting Enable:
6 (Packets)

抓包信息：
1/0/13口有3个DHCP Discover报文，1/0/14口无该MAC地址报文



从抓包信息来看，确未看到2/0/14口的DHCP Discover报文，看起来很像是设备把报文丢了。进一步看下设备底层丢包统计信息。

2、通过诊断信息查看设备有无底层丢包信息

底层有大量RDBGC7.ge14 丢包，RDBGC7表示端口STP block丢包计数，ge14表示端口2/0/13。

RDBGC7.ge14 : 17+18,446,744,073,709,551,567

==========debug port mapping 1==========

==========

[Interface] [Unit][Port][Name][Combo?][Active?][IfIndex] [MID][Link] [Attr]

==========

GE1/0/1 0 3 ge2 no no 0x900000 2 down Bridge

GE1/0/2 0 2 ge1 no no 0x900001 2 down Bridge

GE1/0/13 0 15 ge14 no no 0x90000c 2 up Bridge

芯片底层未见拥塞丢包，只有1/0/13口STP丢包记录。怀疑现场问题域13口STP状态相关，查看操作记录。

3、查看操作记录

%Apr 28 04:26:04:209 2000 BJW2-A088/A087-37-PR-SW SHELL/6/SHELL_CMD: -Task=vt0-IPAddr=10.13.1.1-User=admin; Command is display qos policy interface

%Apr 28 04:26:20:581 2000 BJW2-A088/A087-37-PR-SW MSTP/6/MSTP_FORWARDING: Instance 0's port GigabitEthernet1/0/13 has been set to forwarding state.

从记录看stp的状态都没有切换成forwarding，就开始测试了，端口up后，需要30s，stp才会forwarding

Server侧未见抓包怀疑是端口1/0/13口还未forwarding所致，之前流统计一直没有报文也是这个原因。

client侧抓包发现该源MAC的DHCP Discover报文也只有3个，说明该报文没有一直发送，而这三个报文都是非forwarding状态发送的，被丢弃导致地址获取失败。

连接终端的端口配置为stp-edged 端口+BPDU保护。

现场问题产生的原因有两点：

（1）设备开启STP，端口正常参与数据转发需要等待30s

（2）现场问题终端网卡UP后，不会一直发送DHCP Discover报文

对于网卡的机制，我们无法左右，但对于配置的规范化我们可以掌控。像连接终端的端口，设备开启STP的情况下，建议这些口要配成stp-edged 端口+BPDU保护。