dhcp中继设备割接导致下挂终端无法获取地址地址

DHCP/DHCP Relay 赵阳 2021-10-29 发表

组网及说明

DHCPserver——防火墙——路由器透传——75X（做DHCPrelay）——下挂多个OLT——每个OLT下挂数百个ONU终端

问题描述

局点使用7503X替换之前的CE3000进行割接，割接后发现配置不变的情况下，部分dhcp客户端无法获取地址。

过程分析

1、 查看设备配置：

设备侧配置直接继承CE3000，经检查，配置为正常DHCP中继设置无异常，鉴于是部分终端拿不到地址，怀疑dhcp报文存在拥塞丢包或者环路丢包，但debug查看底层信息发现软件dhcp丢包计数为0，排除dhcp报文过多产生拥塞的可能性，并且现场拓扑信息收集检查过后，确认没有环路问题。

```
#
interface Vlan-interface3291
 ip address XXX
 igmp enable
 dhcp select relay
 dhcp relay server-address XXX
 dhcp relay server-address XXX
#
ID  Type                 RcvPps Rcv_All   DisPkt_All Pps  Dyn Swi Hash ACLmax
34  DHCP_CLIENT          0      3         0          100  S   On  SMAC 8
35  DHCP_SERVER          0      0         0          100  S   On  SMAC 8
36  DHCP_RELAY_CLIENT    0      0         0          300  S   On  SMAC 8
37  DHCP_RELAY_SERVER    22     313454    0          300  S   On  SMAC 8
#
```

2、抓包检查：

后面工程师去往现场进行测试，发现终端无法获取地址并非个别现象，而是所有以7503X设备为中继的客户端均无法获取地址，之前认为是偶发现象的原因是：大多数终端的地址租约尚未到期，因此未发送request或者discover报文进行续约或者重新获取地址。

现场工程师进行抓包排查，发现服务器无法收到任何7503X发出的报文，但于7503X上行路由器设备依旧能够抓到7503X发出的报文，推测为被防火墙策略所拦截，因此分别抓取7503X与CE3000的报文进行比对，发现二者报文差异：CE3000设备做中继时，发出的discover报文源地址为中继接口地址，7503X设备做中继时，发出的discover报文源地址为出接口地址。

7503X设备做中继时的抓包：

5 6.676796	10.167.87.1	192.168.6.111	DHCP	344 DHCP Discover
6 6.676956	10.167.87.1	192.168.6.110	DHCP	344 DHCP Discover

CE3000设备做中继时的抓包：

19 22.759013	10.164.4.1	192.168.6.110	DHCP	363 DHCP Discover
20 22.759277	10.164.4.1	192.168.6.111	DHCP	363 DHCP Discover

由于本差异，因此7503X设备做中继时，dhcp报文被防火墙认为非法并进行拦截，后通过于7503X设备上配置dhcp relay source-address (指定该IP地址为发送到DHCP服务器的报文源地址和giaddr字段)，可以申请到地址，现场恢复正常。（后面通过多个实验，确认较老的设备实现机制都是以做relay的vlan虚接口地址为源IP，由DHCP控制，较新的设备则是以出接口做源IP，由转发控制）

解决方法

通过于7503X设备上配置dhcp relay source-address (指定该IP地址为发送到DHCP服务器的报文源地址和giaddr字段)，可以申请到地址，现场恢复正常。