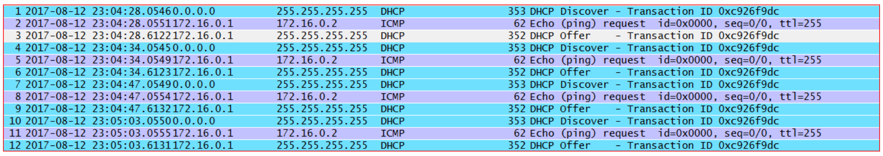
在V7 防火墙上放通dhcp client到dhcp server的域间策略时，客户端者获取不到地址

DHCP　**李超**　2017-08-15 发表

客户组网如下：
DHCP客户端----------FW（二层透传）----------DHCP服务器
用户反馈在FW上只放通dhcp client到dhcp server的域间策略时，客户端获取地址很慢或者获取不到地址。

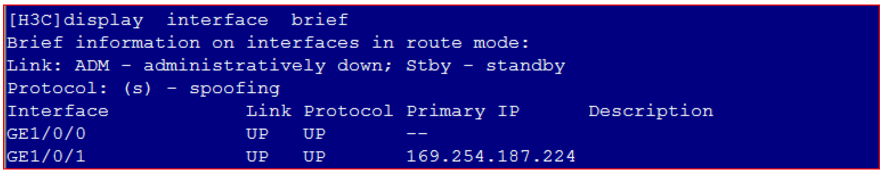
无

1、在FW上只放通dhcp client到dhcp server的域间策略时，服务器回应的dhcp offer报文为广播报文，因没有正向会话而被域间策略丢弃，故客户端无法获取到IP地址。
报文信息如下：



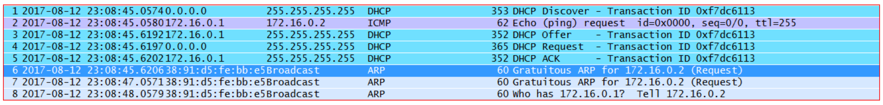
```
 1 2017-08-12 23:04:28.05460.0.0.0          255.255.255.255  DHCP     353 DHCP Discover - Transaction ID 0xc926f9dc
 2 2017-08-12 23:04:28.0551172.16.0.1       172.16.0.2       ICMP      62 Echo (ping) request  id=0x0000, seq=0/0, ttl=255
 3 2017-08-12 23:04:28.6122172.16.0.1       255.255.255.255  DHCP     352 DHCP Offer    - Transaction ID 0xc926f9dc
 4 2017-08-12 23:04:34.05450.0.0.0          255.255.255.255  DHCP     353 DHCP Discover - Transaction ID 0xc926f9dc
 5 2017-08-12 23:04:34.0549172.16.0.1       172.16.0.2       ICMP      62 Echo (ping) request  id=0x0000, seq=0/0, ttl=255
 6 2017-08-12 23:04:34.6123172.16.0.1       255.255.255.255  DHCP     352 DHCP Offer    - Transaction ID 0xc926f9dc
 7 2017-08-12 23:04:47.05490.0.0.0          255.255.255.255  DHCP     353 DHCP Discover - Transaction ID 0xc926f9dc
 8 2017-08-12 23:04:47.0554172.16.0.1       172.16.0.2       ICMP      62 Echo (ping) request  id=0x0000, seq=0/0, ttl=255
 9 2017-08-12 23:04:47.6132172.16.0.1       255.255.255.255  DHCP     352 DHCP Offer    - Transaction ID 0xc926f9dc
10 2017-08-12 23:05:03.05500.0.0.0          255.255.255.255  DHCP     353 DHCP Discover - Transaction ID 0xc926f9dc
11 2017-08-12 23:05:03.0555172.16.0.1       172.16.0.2       ICMP      62 Echo (ping) request  id=0x0000, seq=0/0, ttl=255
12 2017-08-12 23:05:03.6131172.16.0.1       255.255.255.255  DHCP     352 DHCP Offer    - Transaction ID 0xc926f9dc
```

Debug信息如下：（debugging aspf packet acl 3999）
*Aug 12 15:13:58:061 2017 H3C ASPF/7/PACKET: -COntext=1; The first packet was dropped by packet filter or object-policy. Src-ZOne=server, Dst-ZOne=client;If-In=GigabitEthernet1/0/11(12), If-Out=GigabitEthernet1/0/10(11), VLAN-In=200, VLAN-Out=200; Packet Info:Src-IP=172.16.0.1, Dst-IP=172.16.0.2, VPN-Instance=none,Src-Port=0, Dst-Port=2048. Protocol=ICMP(1).
*Aug 12 15:13:58:627 2017 H3C ASPF/7/PACKET: -COntext=1;The packet that matches no session was dropped by packet filter or object-policy. Src-ZOne=server, Dst-ZOne=client;If-In=GigabitEthernet1/0/11(12), If-Out=GigabitEthernet1/0/10(11), VLAN-In=200, VLAN-Out=200; Packet Info:Src-IP=172.16.0.1, Dst-IP=255.255.255.255,VPN-Instance=none, Src-Port=67, Dst-Port=68. Protocol=UDP(17).
当客户端长时间无法获取地址时，接口上会有一个169.254.x.x的地址，表示客户端无法得到DHCP的响应：



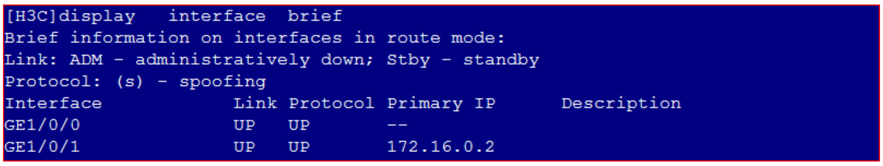
```
[H3C]display  interface  brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE1/0/0              UP   UP       --
GE1/0/1              UP   UP       169.254.187.224
```

2、在防火墙上同时放通dhcp client到dhcp server、dhcp server到dhcp client的域间策略时，客户端可以正常获取IP地址，DHCP交互过程如下：



```
1 2017-08-12 23:08:45.05740.0.0.0          255.255.255.255  DHCP     353 DHCP Discover - Transaction ID 0xf7dc6113
2 2017-08-12 23:08:45.0580172.16.0.1       172.16.0.2       ICMP      62 Echo (ping) request  id=0x0000, seq=0/0, ttl=255
3 2017-08-12 23:08:45.6192172.16.0.1       255.255.255.255  DHCP     352 DHCP Offer    - Transaction ID 0xf7dc6113
4 2017-08-12 23:08:45.61970.0.0.0          255.255.255.255  DHCP     365 DHCP Request  - Transaction ID 0xf7dc6113
5 2017-08-12 23:08:45.6202172.16.0.1       255.255.255.255  DHCP     352 DHCP ACK      - Transaction ID 0xf7dc6113
6 2017-08-12 23:08:45.620638:91:d5:fe:bb:e5Broadcast        ARP       60 Gratuitous ARP for 172.16.0.2 (Request)
7 2017-08-12 23:08:47.057138:91:d5:fe:bb:e5Broadcast        ARP       60 Gratuitous ARP for 172.16.0.2 (Request)
8 2017-08-12 23:08:48.057938:91:d5:fe:bb:e5Broadcast        ARP       60 Who has 172.16.0.1?  Tell 172.16.0.2
```

客户端可以正常获取到ip：



```
[H3C]display  interface  brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE1/0/0              UP   UP       --
GE1/0/1              UP   UP       172.16.0.2
```

该情况下，需要在防火墙上面同时dhcp client到dhcp server和dhcp server到dchp client的域间策略，为了网络的安全，建议配置明细的域间策略。