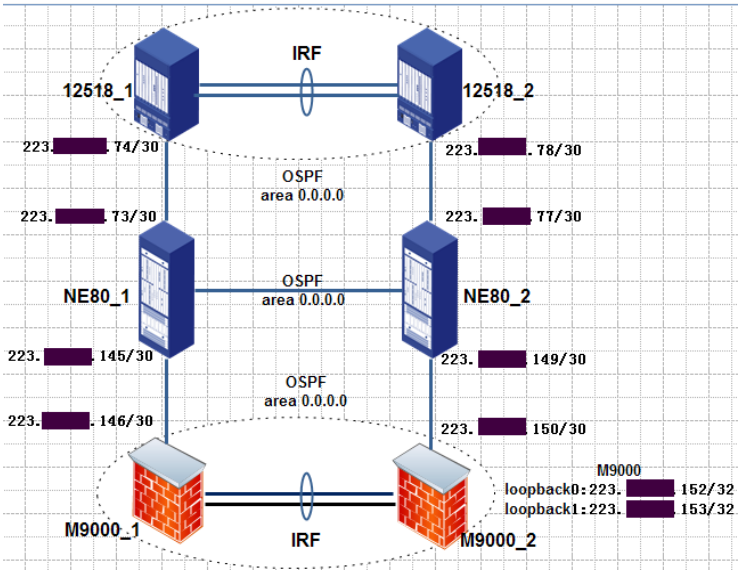
M9000与对端设备ospf不通问题排查举例

域间策略/安全域 屈剑峰 2016-04-28 发表

在M9000上带loopback接口ip地址去ping对端华为NE80设备上与12518互联的ip地址，有的可ping通有的ping不通。



[M9000]ping –a 223.xx.xx.152 223.xx.xx.73
Ping 223.xx.xx.73 (223.xx.xx.73) from 223.xx.xx.152: 56 data bytes, press CTRL_C to break
Request time out
[M9000]ping –a 223.xx.xx.152 223.xx.xx.78
Ping 223.xx.xx.78 (223.xx.xx.78) from 223.xx.xx.152: 56 data bytes, press CTRL_C to break
56 bytes from 223.xx.xx.78: icmp_seq=0 ttl=254 time=1.112 ms

1. 首先排查一下路由情况，查看ospf路由学习是否正确。

M9000 ospf路由配置：

```
ospf 1 router-id 223.xx.xx.152
 import-route static type 1 route-policy policy-cmnet
 filter-policy route-policy policy-default import
 area 0.0.0.0
  network 223. xx.xx.144 0.0.0.3
  network 223. xx.xx.148 0.0.0.3
  network 223.xx.xx.152 0.0.0.0
```

华为NE80路由配置：

```
ospf 1
 default-route-advertise always type 1
 area 0.0.0.0
  network 111. xx.xx.208 0.0.0.7
  network 183. xx.xx.8 0.0.0.3
  network 221. xx.xx.164 0.0.0.3
  network 223. xx.xx.16 0.0.0.3
  network 223. xx.xx.56 0.0.0.3
```

2. 在M9000上查看是否有icmp会话信息，如果没有建议排查域间策略;如果有会话信息，查看是否有icmp响应报文，如果没有建议排查是被M9000丢弃还是对端没有回应。

```
[M9000]dis session table ipv4 destination-ip 223.xx.xx.73 verbose
CPU 1 on slot 0 in chassis 1:
Total sessions found: 0
CPU 1 on slot 1 in chassis 1:
Initiator:
  Source      IP/port: 223.xx.xx.152/39162
  Destination IP/port: 223.xx.xx.73/2048
  DS-Lite tunnel peer: -
```

VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: ICMP(1)
Inbound interface: InLoopBack0
Source security zone: Local
Responder:
Source IP/port: 223.xx.xx.73/39162
Destination IP/port: 223.xx.xx.152/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: ICMP(1)
Inbound interface: Route-Aggregation2.10
Source security zone: Untrust_CMNET
State: ICMP_REQUEST
Application: OTHER
Start time: 2016-04-14 18:02:24 TTL: 40s
Initiator->Responder: 4 packets 336 bytes
Responder->Initiator: 0 packets 0 bytes

以上情况建议排查响应报文是被M9000丢弃还是对端没有回应。

3. 通过命令debugging aspf packet acl xxx可以看报文是否被aspf模块drop掉，及被drop的原因。

*Apr 14 18:14:31:614 2016 SCCD-PS-PCRP-FW001-M9014-IRF ASPF/7/PACKET: -Chassis=1-Slot=1.1; The packet was dropped by ASPF zone change check for nonexistent zone pair. Src-Zone=Untrust_CMNET, Dst-Zone=Untrust_CMNET;If-In=Route-Aggregation2.10(4997), If-Out=Route-Aggregation2.10(4997); Packet Info:Src-IP=223.87.85.146, Dst-IP=223.xx.xx.73, VPN-Instance=none,Src-Port=39218, Dst-Port=2048. Protocol=ICMP(1).
通过debug aspf发现icmp响应报文被ASPF模块drop掉。

4. 通过命令debug ip packet acl xxx 查看报文发送和接收情况，可以查看报文从哪个接口发送出去，哪个接口接收响应报文。

*Apr 14 20:38:53:394 2016 SCCD-PS-PCRP-FW001-M9014-IRF IPFW/7/IPFW_PACKET: -Chassis=1-Slot=0.1;
Sending, interface = Route-Aggregation2.10, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 56502, offset = 0, ttl = 255, protocol = 1,
checksum = 44892, s = 223.xx.xx.152, d = 223.xx.xx.78
prompt: Sending the packet from local at Route-Aggregation2.10.

*Apr 14 20:38:53:394 2016 SCCD-PS-PCRP-FW001-M9014-IRF IPFW/7/IPFW_PACKET: -Chassis=1-Slot=0.1;
Receiving, interface = Route-Aggregation1.10, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 29825, offset = 0, ttl = 254, protocol = 1,
checksum = 6290, s = 223.xx.xx.78, d = 223.xx.xx.152
prompt: Receiving IP packet.

5. 通过debug ip info acl xxx查看报文转发信息

*Apr 14 20:42:50:490 2016 SCCD-PS-PCRP-FW001-M9014-IRF IPFW/7/IPFW_INFO:
MBUF was intercepted! Phase Num is 7, Service ID is 0, Bitmap is a000000000000000, return 2!
Interface is Route-Aggregation2.10,s= 223.xx.xx.152, d= 223.xx.xx.78, protocol= 1, pktid = 60415.

6. 流统计

确认了域间策略没有问题且报文被ASPF模块drop掉情况下，可通过流统计方式查看报文的收发情况。
在接口进行包数统计，一般ping包进行测试，发出多少imcp请求，根据接口统计响应多少icmp报文。
请求数和响应包数一样，说明对端设备没有丢包。如果接收的响应报文数少说明对端设备存在问题，
如果接收的响应报文数多与请求报文数，有可能环路导致或者其他原因，建议排查对端设备。

l 配置CB对策略

[M9000]traffic classifier icmptest
[M9000-classifier-icmptest]if-match acl 3999

```
[M9000]traffic behavior icmptest
[M9000-behavior-icmptest] accounting


[M9000]qos  policy  icmptest
[M9000-qospolicy-icmptest]classifier  icmptest  behavior  icmptest

    l 接口应用qos policy策略
[M9000-Ten-GigabitEthernet2/12/0/1]qos  apply  policy  icmptest inbound  enhancement

    l 查看接口流统计结果，发现ping对端5个报文，却收到对端635个响应报文。
[M9000]ping  -a 223.xx.xx.152 223.xx.xx.73
[M9000]dis qos  policy  interface  Ten-GigabitEthernet  2/12/0/1
Interface: Ten-GigabitEthernet2/12/0/1
  Direction: Inbound
  Type     : Enhancement
  Policy: icmptest
   Classifier: default-class
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: icmptest
     Operator: AND
     Rule(s) :
      If-match acl 3999
     Behavior: icmptest
      Accounting enable:
        635 (Packets)

    l 如果带ttl值为7去ping，发现收到对端30个响应报文。
< M9000>ping -h 7 -a 223.xx.xx.152 223.xx.xx.73
< M9000>dis qos policy interface Ten-GigabitEthernet 2/12/0/1
Interface: Ten-GigabitEthernet2/12/0/1
  Direction: Inbound
  Type     : Enhancement
  Policy: icmptest
   Classifier: default-class
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: icmptest
     Operator: AND
     Rule(s) :
      If-match acl 3999
     Behavior: icmptest
      Accounting enable:
        30 (Packets)
    l 带ttl值为30去ping，发现收到对端75个响应报文。
< M9000>ping -h 30 -a 223.xx.xx.152 223.xx.xx.73
< M9000>dis qos policy interface Ten-GigabitEthernet 2/12/0/1
Interface: Ten-GigabitEthernet2/12/0/1
  Direction: Inbound
  Type     : Enhancement
  Policy: icmptest
   Classifier: default-class
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
```

-none-
Classifier: icmptest
Operator: AND
Rule(s) :
If-match acl 3999
Behavior: icmptest
Accounting enable:
75 (Packets)

经过排查发现，发现M9000收到对端icmp响应的报文数多于icmp请求数，综合分析初步诊断应该是对端路由环路原因导致的，建议排查对端路由配置。

排查命令汇总

1. display session table ipv4 destination-ip 223.xx.xx.73 verbose
2. debugging aspf packet acl xxx
3. debug ip packet acl xxx
4. ping -h [n] -a [Sip] [Dip]
5. traffic classifier icmptest
   if-match acl 3999
6. traffic behavior icmptest
   accounting
7. qos policy icmptest
   classifier icmptest behavior icmptest

常用的ping参数（有助于问题定位）

ping -c 100 -s 100 -h 1 -i M-GigabitEthernet 1/0/0/0 -r -a 172.31.0.18 172.31.0.1

-a 带原地址ping
-c 自定义ping包数
-h 自定义ttl值
-i 指定ping出接口
-r ping同时记录路由信息
-s 自定义ping包大小
-vpn-instance 带vpn实例ping