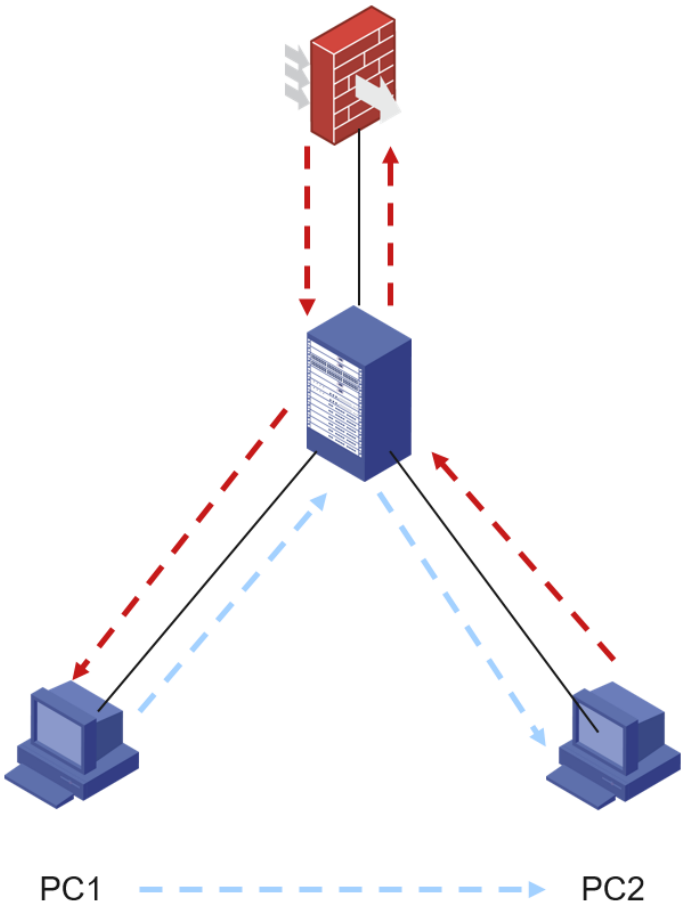
某局点S7503X IRF环境下挂2个终端三层互访不通的经验案例

策略路由 张腾 2021-09-26 发表

组网及说明



如图2台S7503X做IRF作为2个终端的网关，PC1和PC2不同网段。PC1访问PC2的流量，去方向直接通过交换机发往PC2，PC2的回城流量通过策略路由引到第三方准入设备后再发给S7503X，然后发给PC1。

问题描述

PC1访问PC2不通

过程分析

1、在S7503X上部署流量统计，发现PC1访问PC2的回城流量从准入设备发给S7503X后，S7503X未回给PC1。

```
Interface: Ten-GigabitEthernet2/2/0/34
 Direction: Inbound
 Policy: liutong
  Classifier: liutong
    Operator: AND
    Rule(s) :
     If-match acl 3333
    Behavior: liutong
     Accounting enable:
       4 (Packets)
       0 (pps)

Interface: Ten-GigabitEthernet2/2/0/34
 Direction: Outbound
 Policy: liutong
  Classifier: liutong
    Operator: AND
    Rule(s) :
     If-match acl 3333
    Behavior: liutong
     Accounting enable:
       0 (Packets)
       0 (pps)

dis qos poli in ten2/2/0/33
Interface: Ten-GigabitEthernet2/2/0/33
 Direction: Inbound
 Policy: liutong
  Classifier: liutong
    Operator: AND
    Rule(s) :
     If-match acl 3333
    Behavior: liutong
     Accounting enable:
       4 (Packets)
       0 (pps)

Interface: Ten-GigabitEthernet2/2/0/33
 Direction: Outbound
 Policy: liutong
  Classifier: liutong
    Operator: AND
    Rule(s) :
     If-match acl 3333
    Behavior: liutong
     Accounting enable:
       4 (Packets)
       0 (pps)

dis qos poli in ten1/2/0/26
Interface: Ten-GigabitEthernet1/2/0/26
 Direction: Inbound
 Policy: liutong
  Classifier: liutong
    Operator: AND
    Rule(s) :
     If-match acl 3333
    Behavior: liutong
```

```
    Accounting enable:
      4 (Packets)
      0 (pps)
Interface: Ten-GigabitEthernet1/2/0/26
  Direction: Outbound
  Policy: liutong
   Classifier: liutong
     Operator: AND
     Rule(s) :
      If-match acl 3333
     Behavior: liutong
      Accounting enable:
       4 (Packets)
       0 (pps)
```

2、PC2回城流量的转发路径如下：

PC2--->2/2/0/34--->PBR--->1/2/0/26--->准入设备---->1/20/26---->2/2/0/33---->PC1

通过部署内部HG流统，并且用PC2来pingPC1来看PC2发起的ICMP request报文从准入设备回来后，已经通过堆叠口送到2框了。但是没有从2/2/0/33口发出去。

3、将2框堆叠口报文镜像到CPU，发现ICMP request报文的目的是1/2/0/26口，而不是正常的2/3/0/33口

```
drv_rxtx_rx():unit=0,
port=40,pvlan=60,cos=2,reason=0x0,length=78,sMod=4,sPort=27,dMod=4,dPort=27,opcode=1,rxMatched=0,rx_untagged=3,uiDrvRxFlags=0x44,srcvp=4294967295,mcgroup=1051,reasOns=0x0000 0000 0000 0000 0000 0000 0000 ,hghdr: fb 00 04 1b 04 1b 3b 00 21 00 00 00 00 3c 01 00
*Sep 10 20:24:16:236 2021 S7003X DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=2-Slot=2;
From board 20: received packet from
chip0,port40,reason=0x0,cos=2,sMod=4,sPort=27,len=78,Matched=0,time=0,src_vp=-1
*Sep 10 20:24:16:236 2021 S7003X DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=2-Slot=2;
 -----------------------------------------------------
0000  40 6c 8f b8 d1 5f 9c 54 c2 08 1c 01 81 00 00 3c
 0010  08 00 45 00 00 3c 24 9d 00 00 3e 01 d2 79 ac 14
 0020  f1 01 ac 14 3c 80 08 00 2c c5 00 01 20 96 61 62
```

解析报文描述符资源，目的也是1/2/0/26口

```
[S7003X-probe]bcm c 2 s 2 c 0 h2higig2/0xfb00041b/0x041b3b00/0x21000000/0x003c0100
0xfb00041b <START=0xfb MCST=0x0 TC=0 DST_MOD=4 DST_PORT=27
           OVERLAY: MGID=1051>
0x041b3b00 <SRC_MOD=4 SRC_PORT=27 LBID=59 DP=0 EHV=0 PPD_TYPE=0>
0x21000000 <DST_T=0 DONOT_MODIFY=0 DONOT_LEARN=1
            LEG_FAILOVER=0 IT=0 MO=0 MD=0 M=1 L3=0
           LP=0 LABEL_TYPE=0 VC_LABEL=0x00000
           REPLICATION_ID=0x0>
0x003c0100 <VLAN_PRI=0 VLAN_CFI=0 VLAN_ID=60
           PFM=0 SRC_T=0 PRESERVE_DSCP=0
           PRESERVE_DOT1P=0 OPCODE=1 HXL=0>
 0030  63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
 0040  73 74 75 76 77 61 62 63 64 65 66 67 68 69
```

4、PC2的网关接口配置了PBR，下一跳出接口就是1/2/0/26口。正常情况下从准入发过来的三层流量不会再匹配PBR，但从现象看从准入发给S7503X的报文又匹配了PBR。将网关接口的PBR配置删除后，出接口正确，PC1和PC2能够正常通信。

```
[S7003X-Vlan-interface60]undo ip policy-based-route
*Sep 10 20:39:37:941 2021 S7003X DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=2-Slot=2;
 drv_rxtx_rx():unit=0, port=40,pvlan=60,cos=2,reason=0x0,length=78,sMod=4,sPort=27,dMod=36,dPort=34,opcode=1,rxMatched=0,rx_untagged=3,uiDrvRxFlags=0x44,srcvp=4294967295,mcgroup=9250,reasOns=0x0000 0000 0000 0000 0000 0000 0000 ,hghdr: fb 00 24 22 04 1b 3b 00 21 00 00 00 00 3c 01 00
*Sep 10 20:39:37:941 2021 S7003X DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=2-Slot=2;
From board 20: received packet from
chip0,port40,reason=0x0,cos=2,sMod=4,sPort=27,len=78,Matched=0,time=0,src_vp=-1
*Sep 10 20:39:37:941 2021 S7003X DRVPLAT/7/RxTxDebug: -MDC=1-Chassis=2-Slot=2;
 -----------------------------------------------------
0000  40 6c 8f b8 d1 5f 9c 54 c2 08 1c 01 81 00 00 3c
 0010  08 00 45 00 00 3c 24 a0 00 00 3e 01 d2 76 ac 14
 0020  f1 01 ac 14 3c 80 08 00 2c c2 00 01 20 99 61 62
```

解决方法

改成MQC实现需求：

```
#创建acl规则
acl number 3100
 rule 0 permit ip source 60.0.0.2 0 destination 70.0.0.2 0
 rule 5 permit ip source 70.0.0.2 0 destination 60.0.0.2 0
#
 #配置MQC
traffic classifier test operator and
 if-match acl 3100
 if-match forwarding-layer route
 if-match destination-mac 48bd-3d25-1001  //这个目的mac是750X3设备上VLAN虚接口的mac地址
#
traffic behavior test
redirect next-hop 110.0.0.2
#
qos policy test
classifier test behavior test
#
 #全局下发vlan 下的MQC
qos vlan-policy test vlan 60 inbound
```

```
0030  63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
0040  73 74 75 76 77 61 62 63 64 65 66 67 68 69
```