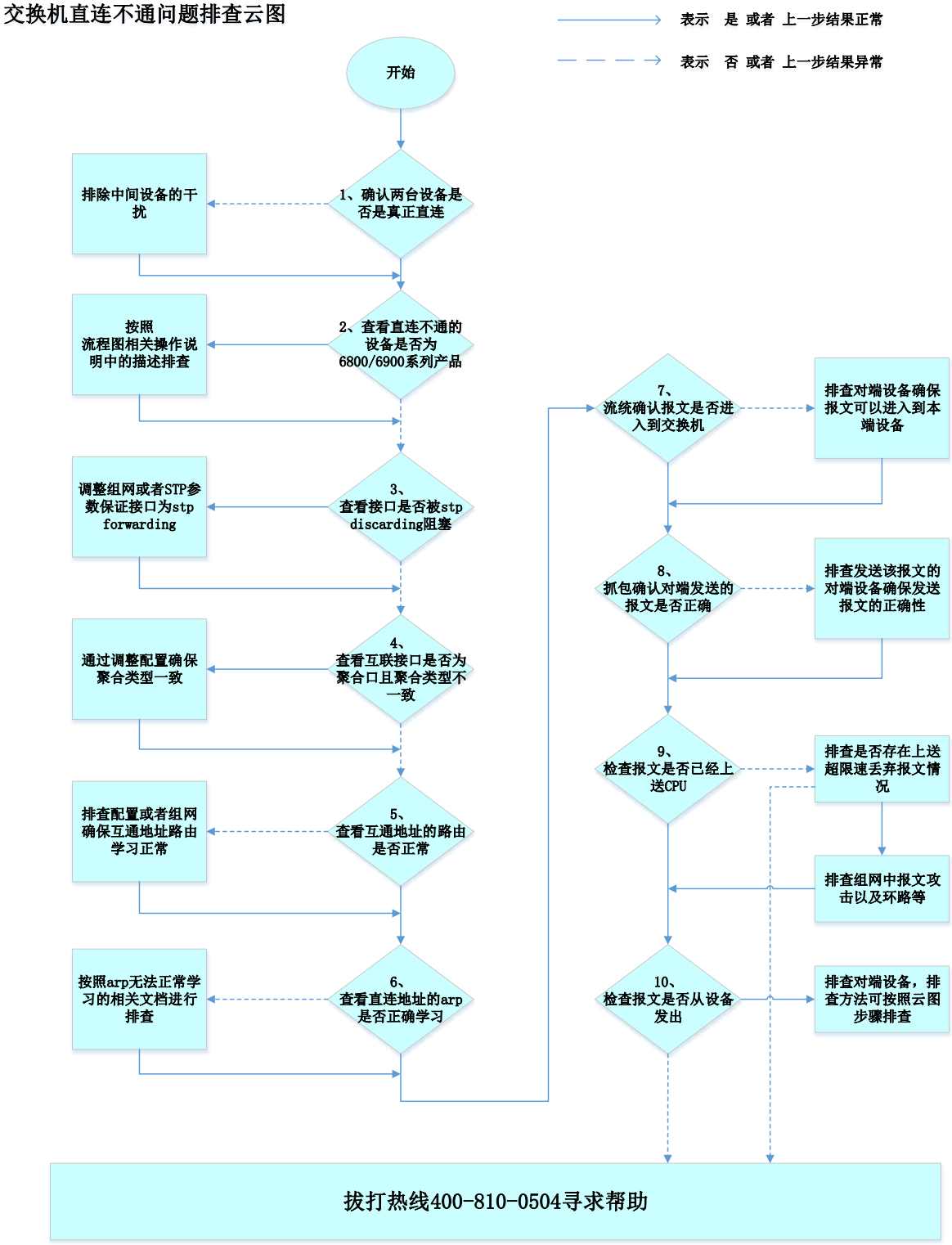
交换机直连不通问题排查云图



一、开始

在交换机开局和维护中，直连不通是一类较为常见的问题。

排查交换机直连不通问题时，一般都通过两个设备互 ping 的方式来测试。如果互 ping 发现直连不通。首先要现场明确两个设备是否是真正的直连，即两个设备之间是否还有其他设备，因为经常会遇到有中间设备将报文丢弃的场景，如果确认两个设备是真正的直连，接下来则需要排查是否因为聚合、STP、路由、arp 以及产品本身问题等导致的直连不通的情况。

具体排查思路如下：

1. **步骤 1**：首先要现场明确两个设备是否是真正的直连，即两个设备之间是否还有其他中间设备。如果有中间设备，请排除掉中间设备的干扰，如果无其它中间设备，进入步骤 2 继续排查。
2. **步骤 2**：查看直连不通的设备是否为 6800/6900 系列产品，如果是的话请按照流程图相关操作说明中的描述排查，如果不是的话，则进入第 3 步继续排查。
3. **步骤 3**：查看接口是否被 stp discarding 阻塞，如果被 stp 阻塞，请调整组网或者 STP 参数保证接口为 stp forwarding，如果 stp 状态为 forwarding，则进入步骤 4 继续排查。
4. **步骤 4**：查看互联接口是否为聚合口且聚合类型不一致，如果是的话，则通过调整配置确保聚合类型一致，如果不存在该情况，则进入步骤 5 继续排查。
5. **步骤 5**：通过 display ip routing-table 查看直连互通地址的路由是否正确，如果不正确请排查配置或者组网确保互通地址路由学习正常，如果路由正确，则进入第 6 步继续排查。
6. **步骤 6**：查看直连地址的 arp 是否学习正确，如果不正确，请按照 arp 无法正常学习的相关文档进行排查，如果 arp 学习正常，则进入步骤 7 进一步排查。
7. **步骤 7**：流统确认报文是否进入到交换机，如果未进入到交换机，则排查对端设备，如果流统确认报文已进入到设备，则进入第 8 步继续排查。
8. **步骤 8**：抓包确认对端发送的报文是否正确，主要检查报文里的源目 mac、vlan 标签、源目 IP 等，如果报文异常，则排查发送该报文的对端设备，如果

报文正常，则进入步骤 9 继续排查。

9. **步骤 9**：检查报文是否已经上送 CPU，如果未上送 CPU，先通过 debug rxtx softcar show slot x 命令查看是否存在 icmp 超限速丢弃的情况，或者有其他协议报文上送 CPU 大量丢弃的情况，如果存在则要排查网络里报文大量上送 CPU 的原因 ,例如是否存在报文攻击、环路等等,如果不存在超限速情况，则拨打 4008100504 反馈分析；若报文已经上送 CPU，则进入第 10 步继续排查。
10. **步骤 10**：检查报文是否从设备发出，可先查看 debugging ip icmp 是否有 output 的报文，如果没有，说明报文未从 CPU 发出，此时请拨打 4008100504 反馈分析，如果有对应的 output 报文，此时需要判断报文是否从对应的接口发出，由于很多设备从 CPU 发出的报文流统不到或者镜像不到，所以可以在对端设备的互联口进行入方向的流统或者镜像，从而确定报文是否从设备发出到对端，如果未发出，此时请拨打 4008100504 反馈分析；如果报文已经从设备发出到了对端设备，但是直连仍不通，如果对端是 H3C 交换机产品，则排查对端设备，排查方法可按照本云图步骤排查。

二、流程图相关操作说明：

1. 确认两台设备是否是真正直连

首先要现场明确两个设备是否是真正的直连，即两个设备之间是否还有其他中间设备。在两台设备开启 LLDP 的情况下,可以先通过 display lldp neighbor-information list 查看是否能看这两台设备的 LLDP 邻居关系，如果不能看到则说明两台设备非直连，此时如果直连不通则需要排除中间设备的影响，如果能看到对应的 LLDP 邻居关系，此时还需要明确现场实际设备连接关系，如果中间设备关闭 LLDP,此时 LLDP 报文是透传的，这时这两个设备还是能看到 LLDP 邻居关系，因此要防止因为该场景造成的误判。在确认两台设备是真正直连的，则进入步骤 2 继续排查。

查看设备 LLDP 邻居关系的命令如下：

```
<H3C>display lldp neighbor-information list
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                 System Name
XGE2/0/3   4ea-c830-5000  Ten-GigabitEthernet1/1/0/1   S12504X-AF-1
XGE2/0/45  74ea-c830-5a00  Ten-GigabitEthernet1/0/15    S12504X-AF-2
FGE2/0/54   f010-90b4-e320    HundredGigE1/0/33          2100-9850
MGE0/0/0    c4ca-d9b9-bb86    GigabitEthernet2/0/7       S5800-56C
```

2. 查看直连不通的设备是否为 6800/6900 系列产品

如果直连不通的设备中有 6800/6900 系列产品，且版本为 25XX/26XX/27XX，则请先查看是否存在如下情况，如果存在则按照如下进行确认，如果不存在，则进入第 3 步继续排查。

配置三层以太网子接口（包括三层路由口子接口或三层聚合子接口）与指定 VPN 实例关联时，至少需要满足以下条件之一：

- 相同子接口编号的三层聚合子接口和 VLAN 接口均与该 VPN 实例关联。
- 在三层以太网子接口下开启以太网子接口的报文统计功能。

该限制表示，子接口编号相同的接口，比如 ragg100.100 和 ragg200.100 的子接口编号都为 100，则如果 ragg100.100 绑定了 VPN 1，那么另一个子接口 ragg200.100 也要绑定 VPN 1，如果因为业务需要，ragg200.100 需要绑定不同的 VPN，比如 VPN2，或者不绑定 VPN，则需要在子接口下配置 traffic-statistic enable。此外，如果设备上起了同编号的 int vlan 接口，比如 int vlan 100，此时 int vlan 100 下也需要绑定一样的 VPN，如果无法绑定的话，则也需要在子接口下配置 traffic-statistic enable。

3. 查看接口是否被 stp discarding 阻塞

客户现网环境一般设备较多，互联线路也较多，此时可能会出现直连的两个

接口中有一个 STP 计算后处于 discarding 状态的情况，因此需要先通过 display stp brief 命令查看接口 STP State 是否是 discarding 的，如果为 discarding，则调整组网或者 STP 的选路，使得互联的接口 STP State 状态为 Forwarding，如果互联接口的 STP 状态均为 Forwarding，则进入步骤 4 继续排查。

查看接口 stp 状态的命令如下：

```
[2015-S12504X-AF]display stp brief
 VLAN ID  Port                        Role  STP State   Protection
 1        Ten-GigabitEthernet1/0/2    DESI  FORWARDING     NONE
 1        Ten-GigabitEthernet1/0/15   DESI  FORWARDING     NONE
 1        Ten-GigabitEthernet1/0/19   ROOT  FORWARDING     NONE
```

4. 查看互联接口是否为聚合口且聚合类型不一致

如果两个直连设备的互联口是聚合口，一定要确认是否一端为动态聚合，另一端为静态聚合，此时会出现动态聚合侧只有一个口默认选中，但是静态聚合侧成员口都选中的情况，由于对端发送的报文通过静态聚合口 hash 时，可能会将报文 hash 到和动态聚合侧非选中端口连接的接口上，从而导致直连不通。如果存在该情况，请修改直连接口的聚合类型，保证两边同为动态聚合或者同为静态聚合，如果修改后依然直连不通或者不存在该情况，则进入步骤 5 继续排查。

由于静态聚合选中端口的规则为，只要接口物理状态 up，且端口和参考端口的属性类配置一致，该端口则会选中，而动态聚合除了需要这些条件外，还需要两个设备可以正常交互 LACP 报文，所以如果一端为动态聚合，一端为静态聚合，在配置正确的情况下，就会出现静态聚合侧端口全部为选中，而动态聚合侧只有一个口默认选中的情况。

查看聚合口是动态聚合口还是静态聚合口的命令为 display link-aggregation verbose。查询到的内容里如果 Aggregation Mode 是 Dynamic，则表示为动态聚合，如果 Aggregation Mode 为 Static，则表示静态聚合。查看接口是否为选中状态通过该命令下的 Status 来确定，如果是 S 表示选中，如果为 U 表示非选中。

```
<H3C> display link-aggregation verbose bridge-aggregation 10
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Aggregate Interface: Bridge-Aggregation10
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
 Port            Status   Priority Index    Oper-Key      Flag
 XGE1/0/1        S        32768    61       2             {ACDEF}
 XGE1/0/2        S        32768    62       2             {ACDEF}
 XGE1/0/3        S        32768    63       2             {ACDEF}
Remote:
 Actor       Priority Index    Oper-Key SystemID               Flag
 XGE1/0/1(R) 32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
 XGE1/0/2    32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
 XGE1/0/3    32768    113      2        0x8000, 000f-e267-57ad {ACDEF}
```

5. 查看互通地址的路由是否正常

直连设备互通时，设备依然是需要通过查询路由来确定是否可以正常互通的，而不是仅仅查看 arp，所以请通过 display ip routing-table 命令查看需要互通的地址的路由协议是否为 Direct，如果是非 Direct，则请排查配置看是否错误配置了针对目的地址的掩码更长的静态路由等，或者排查组网查看该目的地址是否学习成了其他协议类型的路由，如果存在该情况会导致报文无法正确从对应的端口发送出去。如果不存在该情况，则进入步骤 6 继续排查。

举例：

两台交换机 A 与 B 直连，此时 A 设备接口地址为 33.1.1.2，B 设备与 A 设备直连的接口地址为 33.1.1.1，此时在 A 设备上查询路由和 33.1.1.1 的 arp 如下

```
[H3C]display ip routing-table

Destinations : 38       Routes : 38

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24          BGP     255 0           33.1.1.1        XGE1/0/32
1.1.1.3/32          BGP     255 0           33.1.1.1        XGE1/0/32
1.1.1.4/32          BGP     255 0           33.1.1.1        XGE1/0/32
2.2.2.0/24          Direct  0   0           2.2.2.2         XGE1/0/3
2.2.2.0/32          Direct  0   0           2.2.2.2         XGE1/0/3
2.2.2.2/32          Direct  0   0           127.0.0.1       InLoop0
2.2.2.255/32        Direct  0   0           2.2.2.2         XGE1/0/3
5.5.5.5/32          Direct  0   0           127.0.0.1       InLoop0
7.7.7.7/32          Direct  0   0           127.0.0.1       InLoop0
9.1.1.0/24          BGP     255 0           33.1.1.1        XGE1/0/32
10.10.10.0/24       BGP     255 0           33.1.1.1        XGE1/0/32
10.10.10.10/32      BGP     255 0           33.1.1.1        XGE1/0/32
10.10.10.11/32      BGP     255 0           33.1.1.1        XGE1/0/32
13.1.1.0/24         Direct  0   0           13.1.1.2        Vlan3000
13.1.1.0/32         Direct  0   0           13.1.1.2        Vlan3000
13.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
......
13.1.1.255/32       Direct  0   0           13.1.1.2        Vlan3000
33.1.1.0/24         Direct  0   0           33.1.1.2        XGE1/0/32
33.1.1.0/32         Direct  0   0           33.1.1.2        XGE1/0/32
33.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
33.1.1.255/32       Direct  0   0           33.1.1.2        XGE1/0/32

[H3C]display arp 33.1.1.1
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport   I-Invalid
IP address      MAC address     VLAN/VSI   Interface/Link ID     Aging Type
33.1.1.1        4077-a9f0-38fd  --         XGE1/0/32              753   D
```

在 A 设备配置如下静态路由

ip route-static 33.1.1.1 32 2.2.2.1

此时继续在 A 设备上查看路由和 arp 如下。可以发现，arp 学习依然是正常，但是根据最长掩码匹配规则，此时如果用 A 设备 ping 33.1.1.1,报文会从 1/0/3 口出去，会导致直连不通。

```
[H3C]display ip routing-table
Destinations : 32       Routes : 32
Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
2.2.2.0/24          Direct  0   0           2.2.2.2         XGE1/0/3
2.2.2.0/32          Direct  0   0           2.2.2.2         XGE1/0/3
2.2.2.2/32          Direct  0   0           127.0.0.1       InLoop0
2.2.2.255/32        Direct  0   0           2.2.2.2         XGE1/0/3
5.5.5.5/32          Direct  0   0           127.0.0.1       InLoop0
7.7.7.7/32          Direct  0   0           127.0.0.1       InLoop0
13.1.1.0/24         Direct  0   0           13.1.1.2        Vlan3000
13.1.1.0/32         Direct  0   0           13.1.1.2        Vlan3000
13.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
13.1.1.255/32       Direct  0   0           13.1.1.2        Vlan3000
33.1.1.0/24         Direct  0   0           33.1.1.2        XGE1/0/32
33.1.1.0/32         Direct  0   0           33.1.1.2        XGE1/0/32
33.1.1.1/32         Static  60  0           2.2.2.1         XGE1/0/3
33.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
33.1.1.255/32       Direct  0   0           33.1.1.2        XGE1/0/32

[H3C]display arp 33.1.1.1
 Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address     MAC address     VLAN/VSI   Interface/Link ID    Aging Type
33.1.1.1       4077-a9f0-38fd --          XGE1/0/32              359   D

[H3C]ping 33.1.1.1
Ping 33.1.1.1 (33.1.1.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- Ping statistics for 33.1.1.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
[H3C]%Jan 22 14:53:47:232 2011 2064-S6800-54QF PING/6/PING_STATISTICS: Ping
statistics for 33.1.1.1: 5 packet(s) transmitted, 0 packet(s) received,
100.0% packet loss.
```

6. 查看直连地址的 arp 是否正确学习

请通过 display arp 查看设备是否可以学习到对端设备地址的 arp 信息，如果未学习到或者学习 arp 有误，请按照设备无法学习 arp 的相关方法进行排

查，如果已经正常学习到了 arp 但是依然直连不通，则进入步骤 7 继续排查

```
[H3C] display ip routing-table 33.1.1.1

Summary count : 2

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/0          Static  60  0           50.13.0.34      Vlan10
33.1.1.0/24        Direct  0   0           33.1.1.2        XGE1/0/32

[H3C]display arp 33.1.1.1
Type: S-Static    D-Dynamic    O-Openflow    R-Rule    M-Multiport   I-
Invalid
IP address  MAC address  VLAN/VSI  Interface/Link ID    Aging Type
33.1.1.1   4077-a9f0-38fd --       XGE1/0/32             1116  D
```

7. 流统确认报文是否进入到交换机

可以用对端设备或者终端 ping 该交换机，然后在交换机上进行流统，确认报文是否已经进入到设备。流统参考如下举例，更多流统方法请参考《交换那些事儿 | 基础维护篇 - 流统》中的内容，如果流统发现报文未进入到该设备，则排查对端设备或者终端，如果报文进到设备了，则进入第 8 步排查。

以 SWA（1/0/32 33.1.1.2 ）------（33.1.1.1 1/3/2）SWB 直连互通为例。流统配置如下：

```
#
acl advanced 3999
 rule 0 permit icmp source 33.1.1.1 0 destination 33.1.1.2 0
 rule 10 permit icmp source 33.1.1.2 0 destination 33.1.1.1 0
#
traffic classifier c1 operator and
 if-match acl 3999
#
traffic behavior b1
 accounting packet
#
qos policy p1
 classifier c1 behavior b1
#
interface Ten-GigabitEthernet1/0/32
 port link-mode route
 ip address 33.1.1.2 255.255.255.0
 qos apply policy p1 inbound
 qos apply policy p1 outbound
#
用 SWB ping SWA 5 个包
[SWA]display qos policy interface Ten-GigabitEthernet 1/0/32
Interface: Ten-GigabitEthernet1/0/32
  Direction: Inbound
  Policy: p1
   Classifier: c1
     Operator: AND
     Rule(s) :
      If-match acl 3999
     Behavior: b1
      Accounting enable:
        5 (Packets)

Interface: Ten-GigabitEthernet1/0/32
  Direction: Outbound
  Policy: p1
   Classifier: c1
     Operator: AND
     Rule(s) :
      If-match acl 3999
     Behavior: b1
      Accounting enable:
        0 (Packets)
```

注：很多交换机设备从 CPU 发出的包是无法流统到的，因此出方向流统显示为 0，此时要确认是否从接口发出了 replay 报文，可以在对端设备的接口进行入方向流统或者抓包进行确认。

8. 抓包确认对端发送的报文是否正确

以 ICMP 报文为例，需要抓包确认终端发送的 icmp 请求报文的目的 mac 是否为设备对应 int vlan 或者三层接口的 mac 地址，源目 IP 是否正确，以及携带 vlan 标签是否正确（注：PC 抓包时默认会将 vlan 标签删掉，要抓带 vlan tag 报文请对 PC 进行设置保证 PC 可以抓到带 tag 报文），如果报文内容不正确，则排查对端设备，如果报文内容正确，则进入第 9 步继续排查。

当现场无条件进行抓包时，也可采用 mirr to cpu 的方式（接口入方向调用流行为是 mirror-to cpu 的 qos 策略）来将进入到设备的 ICMP 报文打印上送 CPU，然后将打印的报文解析为抓包文件进行查看。

因为上 CPU 的报文可能很多，如果全部打印的话意义不大，只需要按照报文特征选择性的打印即可,比如可以按照报文的源目 MAC 地址、源目 IP 地址、VLAN、报文类型等特征进行过滤。

以步骤 7 中 SWA 与 SWB 直连互通为例，用 SWB 的地址 33.1.1.1 去 ping SWA 的地址 33.1.1.2。先通过 display rxtx sip 33.1.1.1 slot 1（接口入方向 slot 号）以及 display rxtx dip 33.1.1.2 slot 1 命令设置过滤开关，只输出源地址为 33.1.1.1，目的地址为 33.1.1.2 的报文，然后通过 debug rxtx -c Num -s Len pkt Slot_ID 命令将这些报文打印出来，“-c”后面的参数为打印报文的个数，“-s”后面的参数为打印报文的长度。

设备可用于进行过滤的条件包括如下类型，图示以 6800 为例，不同产品可能略有不同。

```
[S6800-54QF-probe]display rxtx ?
  all          All packet
  broadcast    Broadcast packet
  chip         Specify the chip number
  cos          COS
  dest_mac     Dest packet mac
  dip          Dest IP
  dipv6        Dest ipv6
  ecid         ecid
  etype        Packet ethernet type
  iptype       Packet IP type
  length       Pkt len
  matchrule    Rx match rule
  multicast    Multicast packet
  offset       Offset
  port         Port
  rcpu         Rcpu packet
  reason       Receive packet reason
  receive      Receive packet
  send         Send packet
  sip          Source IP
  sipv6        Source ipv6
  source_mac   Source packet mac
  switchflag   Display switch flag
  torx         Show rx timeout
  totx         Show tx timeout
  tsrx         Show rx timestamp
  tstx         Show tx timestamp
  tsverbose    Show verbose timestamp
  unicast      Unicast packet
  vlan         VLAN
  vp           VP packet
  vxlan        Vxlan packet
```

打印上送 CPU 的报文的方法如下：

```
<H3C>t d
The current terminal is enabled to display debugging logs.
<H3C>t m
The current terminal is enabled to display logs.
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]probe
[H3C-probe]display rxtx sip 33.1.1.1 sl 1
[H3C-probe]display rxtx dip 33.1.1.2 sl 1
[H3C-probe]debug rxtx -c 10 pkt sl 1
 Debug RxTx packet is on!
[H3C-probe]*Jan 22 16:07:53:343 2011 2064-S6800-54QF
DRVPLAT/7/RxTxDebug:
From board 1: received packet from
chip0,port32,reason=0x1000,cos=9,sMod=64,sPort=32,len=102,Matched=
0,time=-1090796052,src_vp=15328
*Jan 22 16:07:53:344 2011 2064-S6800-54QF DRVPLAT/7/RxTxDebug:
 ------------------------------------------------------
 0000  9c e8 95 72 a1 52 40 77 a9 f0 38 fd 81 00 00 00
 0010  08 00 45 00 00 54 ba c6 00 00 ff 01 bc dd 21 01
 0020  01 01 21 01 01 02 08 00 ec e7 02 7c 00 00 60 d7
 0030  41 a4 00 0e 7b 0f 08 09 0a 0b 0c 0d 0e 0f 10 11
 ------------------------------------------------------
*Jan 22 16:07:53:345 2011 2064-S6800-54QF DRVPLAT/7/RxTxDebug:
From board 1: received packet from
chip0,port32,reason=0x0,cos=9,sMod=64,sPort=32,len=102,Matched=0,t
ime=-1090796052,src_vp=-1
*Jan 22 16:07:53:345 2011 2064-S6800-54QF DRVPLAT/7/RxTxDebug:
 ------------------------------------------------------
 0000  9c e8 95 72 a1 52 40 77 a9 f0 38 fd 81 00 00 00
 0010  08 00 45 00 00 54 ba c6 00 00 ff 01 bc dd 21 01
 0020  01 01 21 01 01 02 08 00 ec e7 02 7c 00 00 60 d7
 0030  41 a4 00 0e 7b 0f 08 09 0a 0b 0c 0d 0e 0f 10 11
 ------------------------------------------------------
……
 ------------------------------------------------------
*Jan 22 16:07:54:157 2011 2064-S6800-54QF DRVPLAT/7/RxTxDebug:
From board 1: debug RxTx packet is off!
注：由于篇幅限制，如上信息删除了一些中间的打印信息。
```

在打印的内容中，不仅能够看到具体的报文内容，结合 debug port mapping Slot_ID 信息还可以看到这些报文是从哪个端口接收的（chip0,port32,

sMod=64,sPort=32），上 CPU 的优先级是多少（cos=9），以及上送 CPU 的原因（reason=0x0），这些内容对于我们定位问题都很有价值。

使用完毕后注意恢复选择开关：display rxtx all slot-id

如下命令为查看接口内部对应关系的命令。

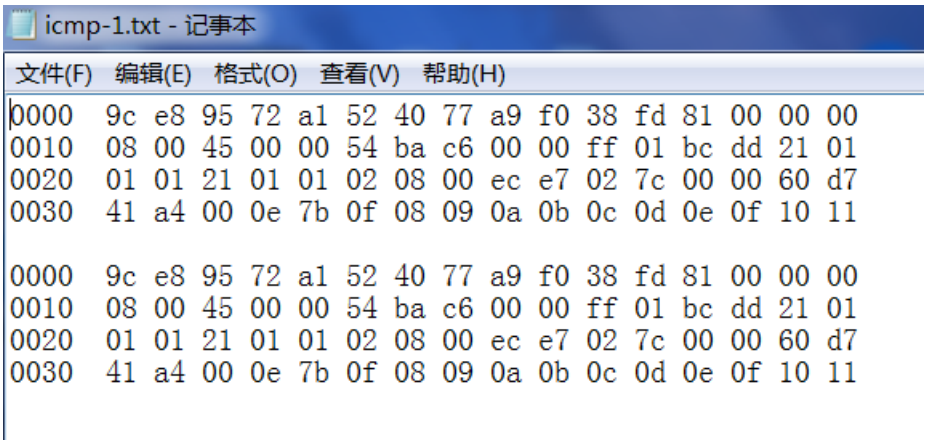
```
[H3C-probe]debug port mapping slot 1

[Interface] [Unit] [Port] [Name] [Combo?] [Active?] [IfIndex] [MID]
[Link] [PipeNum] [PhyAddr]
================================================================================
========================
 XGE1/0/1       0     2      xe1      no          no       0x1         64   up
N/A       N/A
 XGE1/0/2       0     1      xe0      no          no       0x2         64   up
N/A       N/A

……..
 XGE1/0/32     0      32      xe30      no           no        0x20     64   up
N/A       N/A
 XGE1/0/33     0     33     xe31     no          no       0x21      64   down
N/A       N/A
```

虽然有了报文内容，但是却是以十六进制表示的，如果对报文结构不够熟悉，那么就需要进一步通过报文解析软件对这些报文内容进行解析。这里以著名的 Wireshark 为例进行说明。需要手工处理原始的报文打印信息，将报文内容以外的信息去除，处理完成后格式如下：

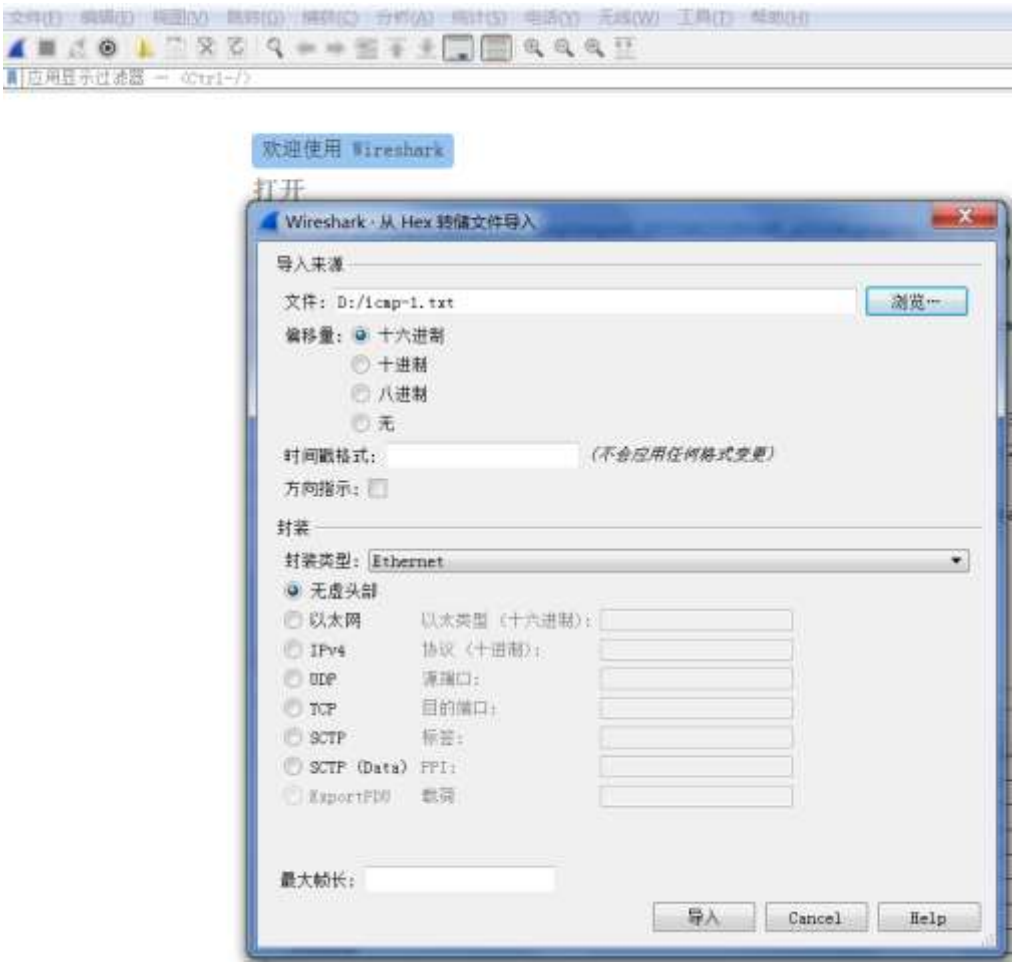
```
0000  9c e8 95 72 a1 52 40 77 a9 f0 38 fd 81 00 00 00
0010  08 00 45 00 00 54 ba c6 00 00 ff 01 bc dd 21 01
0020  01 01 21 01 01 02 08 00 ec e7 02 7c 00 00 60 d7
0030  41 a4 00 0e 7b 0f 08 09 0a 0b 0c 0d 0e 0f 10 11

0000  9c e8 95 72 a1 52 40 77 a9 f0 38 fd 81 00 00 00
0010  08 00 45 00 00 54 ba c6 00 00 ff 01 bc dd 21 01
0020  01 01 21 01 01 02 08 00 ec e7 02 7c 00 00 60 d7
0030  41 a4 00 0e 7b 0f 08 09 0a 0b 0c 0d 0e 0f 10 11
```

将该格式内容保存在 txt 文本里，然后将该 txt 文本文件导入 Wireshark：

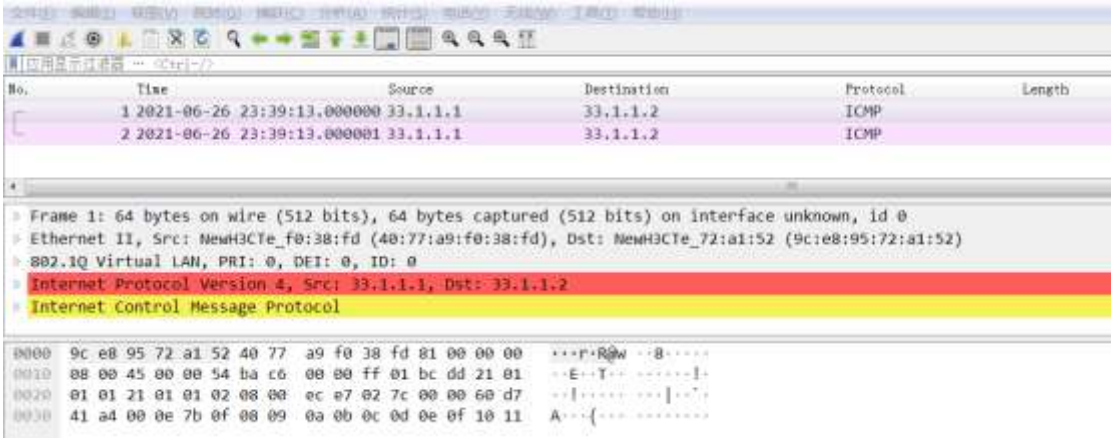
保存的 txt 文本如下



然后打开 wireshark 选择“文件”----“从 Hex 转储导入”，然后“浏览”文件选择刚才保存的 txt 文件。



点击“导入”，此时即会看到解析后的类似于抓包的报文的如下信息。



从抓包可以看出，报文的源 mac 为对端设备的 mac，目的 mac 为本设备的接口 mac，源 IP 和目的 IP 也正确，说明报文内容正确。

```
<H3C>display interface Ten-GigabitEthernet 1/0/32
Ten-GigabitEthernet1/0/32
Current state: UP
Line protocol state: UP
Description: Ten-GigabitEthernet1/0/32 Interface
Bandwidth: 10000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet address: 33.1.1.2/24 (primary)
IP packet frame type: Ethernet II, hardware address: 9ce8-9572-a152
IPv6 packet frame type: Ethernet II, hardware address: 9ce8-9572-
a152
……
<2064-S6800-54QF>disp
<2064-S6800-54QF>display arp 33.1.1.1
  Type: S-Static    D-Dynamic    O-Openflow    R-Rule    M-Multiport
I-Invalid
IP address MAC address    VLAN/VSI    Interface/Link ID    Aging Type
33.1.1.1   4077-a9f0-38fd --          XGE1/0/32              111    D
```

9. 检查报文是否已经上送 CPU

在确认报文已经从接口进到设备后，还需要确认报文是否正常发送到 CPU，因此 ping 设备的报文是需要上送 CPU 处理的。此时可以通过 debugging

ip icmp acl 来进行筛选打印 icmp 报文的 debug 信息。如果有 Input 报文，则表示上送 CPU 了，如果没有，则表示接口进入到设备但未上送 CPU，此时可以先通过 debug rxtx softcar show slot x 命令查看是否存在 icmp 超限速丢弃的情况，或者有其他协议报文上送 CPU 大量丢弃的情况，如果存在则要排查网络里报文大量上送 CPU 的原因，例如是否存在报文攻击、环路等等，如果不存在超限速情况，则拨打 4008100504 反馈分析。

在确定报文已经上送 CPU 后，如果依然直连不通，此时则需要确认报文是否从设备发出，需进入第 10 步骤排查

```
<H3C>dis acl 3999
Advanced IPv4 ACL 3999, 2 rules,
ACL's step is 5, start ID is 0
 rule 0 permit icmp source 33.1.1.1 0 destination 33.1.1.2 0
 rule 10 permit icmp source 33.1.1.2 0 destination 33.1.1.1 0
<H3C>debugging ip icmp acl 3999
<H3C>t d
The current terminal is enabled to display debugging logs.
<H3C>t m
<H3C>*Jan 22 17:03:54:615 2011 2064-S6800-54QF SOCKET/7/ICMP:
ICMP Input:
 ICMP Packet: src = 33.1.1.1, dst = 33.1.1.2
              type = 8, code = 0 (echo)

*Jan 22 17:03:54:615 2011 2064-S6800-54QF SOCKET/7/ICMP:
ICMP Output:
 ICMP Packet: src = 33.1.1.2, dst = 33.1.1.1
              type = 0, code = 0 (echo-reply)

*Jan 22 17:03:54:817 2011 2064-S6800-54QF SOCKET/7/ICMP:
ICMP Input:
 ICMP Packet: src = 33.1.1.1, dst = 33.1.1.2
              type = 8, code = 0 (echo)

*Jan 22 17:03:54:817 2011 2064-S6800-54QF SOCKET/7/ICMP:
ICMP Output:
 ICMP Packet: src = 33.1.1.2, dst = 33.1.1.1
              type = 0, code = 0 (echo-reply)
```

```
[H3C]probe
[H3C-probe]debug rxtx softcar show slot 1
ID   Type              RcvPps Rcv_All     DisPkt_All    Pps   Dyn Swi Hash
ACLmax
0    ROOT                0      160         0          1000 S   On  SMAC 0
1    ISIS                0      0           0          1000 D   On  SMAC 8
2    ESIS                0      0           0          300  S   On  SMAC 8
3    CLNP                0      0           0          300  S   On  SMAC 8
4    VRRP                0      0           0          1000 S   On  SMAC 8
5    UNKNOWN_IPV4MC      0      0           0          300  S   On  SMAC 8
6    UNKNOWN_IPV6MC      0      0           0          300  S   On  SMAC 8
7    IPV4_MC_RIP         0      0           0          500  D   On  SMAC 8
8    IPV4_BC_RIP         0      0           0          500  D   On  SMAC 8
9    MCAST_NTP           0      0           0          300  S   On  SMAC 8
10   BCAST_NTP           0      0           0          300  S   On  SMAC 8
11   IPV4_MC_OSPF_5      0      520611      0          2000 S   On  SMAC 8
12   IPV4_MC_OSPF_6      0      15          0          2000 S   On  SMAC 8
13   IPV4_UC_OSPF        0      0           0          2000 S   On  SMAC 8
14   IPV4_MC_PIM         0      0           0          500  S   On  SMAC 8
15   IPV4_UC_PIM         0      0           0          500  S   On  SMAC 8
16   IPV4_IGMP           1000   387746075   84216529   500  S   On  SMAC 8
……
27   RRPP                0      0           0          300  S   On  SMAC 8
28   IPV4_AUTORP         0      0           0          300  S   On  SMAC 8
29   ARP                 2      188292880   152691765  1000 S   On  SMAC 8
30   ARP_REPLY           0      2121        0          1000 S   On  SMAC 8
31   DHCP_CLIENT         0      0           0          300  S   On  SMAC 8
32   DHCP_SERVER         0      1583        0          300  S   On  SMAC 8
33   DHCP_RELAY_CLIENT   0      0           0          300  S   On  SMAC 8
34   DHCP_RELAY_SERVER   0      0           0          300  S   On  SMAC 8
35   DOT1X               0      0           0          500  S   On  SMAC 8
36   STP                 0      0           0          300  S   On  SMAC 8
37   LACP                0      0           0          300  S   On  SMAC 8
38   GVRP                0      0           0          300  S   On  SMAC 8
39   HGMP                0      0           0          300  S   On  SMAC 8
40   BGP                 0      36986       0          1000 S   On  SMAC 8
41   ICMP                0      2702028     0          500  S   On  SMAC 8
……
```

注：Type 为协议报文类型，RcvPps 为查询该命令时每秒上送 CPU 的报文数，Rcv_All 为该协议报文上送 CPU 的总数，DisPkt_All 由于超限速丢弃的总数，Pps 为设备当前每秒对上送 CPU 报文的限速值。

undo debug rxtx softcar show slot 1 可清除 RcvPps、Rcv_All 和 DisPkt_All 计数。

10.检查报文是否从设备发出

在确认进入到设备的报文上送 CPU 后，可先通过 debugging ip icmp 查看是否有 output 的报文，如果没有，说明报文未从 CPU 发出，此时请拨打 4008100504 反馈分析，如果有对应的 output 报文，仅表示报文从 CPU 发出了，此时仍需要判断报文是否从对应的接口发出了，由于很多设备从 CPU 发出的报文流统不到或者镜像不到，所以可以在对端设备的互联口进行入方向的流统或者镜像，从而确定报文是否从设备发出。如果未发出，此时请拨打 4008100504 反馈分析，如果发出了但是直连仍不通，则排查对端设备，排查方法可按照本云图步骤排查。