H3C MSR 系列路由器

故障处理手册

资料版本：6W101-20221102

目 录

1 简介

本文档介绍 MSR 路由器软、硬件常见故障的诊断及处理措施。

1.1 故障处理注意事项

注意

设备正常运行时，建议您在完成重要功能的配置后，及时保存并备份当前配置，以免设备出现故障后配置丢失。建议您定期将配置文件备份至远程服务器上，以便故障发生后能够迅速恢复配置。

在进行故障诊断和处理时，请注意以下事项：

- 设备出现故障时，请尽可能全面、详细地记录现场信息（包括但不限于以下内容），收集信息越全面、越详细，越有利于故障的快速定位。
  - 记录具体的故障现象、故障时间、配置信息。
  - 记录完整的网络拓扑，包括组网图、端口连接关系、故障位置。
  - 收集设备的日志信息和诊断信息（收集方法见 1.2 收集设备运行信息）。
  - 记录设备故障时单板、电源、风扇指示灯的状态，或给现场设备拍照记录。
  - 记录现场采取的故障处理措施（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
  - 记录故障处理过程中配置的所有命令行显示信息。
- 更换和维护设备部件时，请佩戴防静电手腕，以确保您和设备的安全。
- 故障处理过程中如需更换硬件部件，请参考与软件版本对应的版本说明书，确保新硬件部件和软件版本的兼容性。

1.2 收集设备运行信息

说明

为方便故障快速定位，请使用命令 **info-center enable** 开启信息中心。缺省情况下信息中心处于开启状态。

设备运行过程中会产生 logfile、diagfile 日志信息及记录设备运行状态的诊断信息。这些信息存储在设备的 Flash 或 CF 卡中，可以通过 FTP、TFTP、USB 等方式导出。不同主控板或设备中导出的 logfile、diagfile、诊断信息文件请按照一定规则存放（如不同的文件夹：chassisXslotY），避免不同主控板或设备的运行信息相互混淆，以方便查询。

表1 设备运行信息介绍

分类	文件名	内容
logfile日志	logfileX.log	命令行记录、设备运行中产生的记录信息

diagfile日志	diagfileX.log	设备运行中产生的诊断日志信息，如系统运行到错误流程时的参数值、单板无法启动时的信息、主控板与接口板通信异常时的握手信息。
诊断信息	XXX.gz	系统当前多个功能模块运行的统计信息，包括设备状态、CPU状态、内存状态、配置情况、软件表项、硬件表项等 收集诊断信息会导致设备性能下降，请谨慎使用


说明

对于 logfile 日志和 diagfile 日志，当日志文件写满，产生新的日志文件时，设备会将旧的日志文件自动压缩成.gz 文件。

1.2.2 logfile 日志

(1) 执行 **logfile save** 命令将日志文件缓冲区中的内容全部保存到日志文件中。日志文件缺省存储在存储介质的 logfile 目录中。

```
<Sysname> logfile save
The contents in the log file buffer have been saved to the file
cfa0:/logfile/logfile8.log
```

(2) 查看日志文件的数目和名称。

- 查看设备的 logfile 日志：（集中式设备）

```
<Sysname> dir cfa0:/logfile/
Directory of cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile8.log

1021104 KB total (421552 KB free)
```

- 查看主设备的 logfile 日志：（集中式 IRF 设备）

```
<Sysname> dir flash:/logfile/
Directory of flash:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile.log

1021104 KB total (421552 KB free)
```

- 查看成员设备的 logfile 日志：（集中式 IRF 设备）

```
<Sysname> dir slot2#flash:/logfile/
Directory of slot2#flash:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile.log

1021104 KB total (421552 KB free)
```

- 查看设备主用主控板的 logfile 日志：（分布式设备－独立运行模式）

```
<Sysname> dir cfa0:/logfile/
Directory of cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile8.log

1021104 KB total (421552 KB free)
```

- 查看设备备用主控板的 logfile 日志：（分布式设备－独立运行模式）

```
<Sysname> dir slot1#cfa0:/logfile/
Directory of slot1#cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile8.log

1021104 KB total (421552 KB free)
```

- 查看主设备主用主控板的 logfile 日志：（分布式设备－IRF 模式）

```
<Sysname> dir cfa0:/logfile/
Directory of cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile8.log

1021104 KB total (421552 KB free)
```

- 查看主设备备用主控板的 logfile 日志：（分布式设备－IRF 模式）

```
<Sysname> dir slot1#cfa0:/logfile/
Directory of slot1#cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile8.log

1021104 KB total (421552 KB free)
```

- 查看成员设备主控板的 logfile 日志，如果备设备有两块主控板，则两块都需要检查：（分布式设备－IRF 模式）

```
<Sysname> dir chassis2#slot0#cfa0:/logfile/
Directory of chassis2#slot0#cfa0:/logfile
   0 -rw-       21863 Jul 11 2013 16:00:37   logfile8.log

1021104 KB total (421552 KB free)
```

(3) 使用 FTP、TFTP 或者 USB 接口将日志文件传输到指定位置。

1.2.3 diagfile 日志

(1) 执行 **diagnostic-logfile save** 命令将诊断日志文件缓冲区中的内容全部保存到诊断日志文件中。诊断日志文件缺省存储在存储介质的 diagfile 目录中。

```
<Sysname> diagnostic-logfile save
The contents in the diagnostic log file buffer have been saved to the file
cfa0:/diagfile/diagfile18.log
```

(2) 查看诊断日志文件的数目和名称。

- 查看设备的 diagfile 日志：（集中式设备）

```
<Sysname> dir cfa0:/diagfile/
Directory of cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看主设备的 diagfile 日志：（集中式 IRF 设备）

```
<Sysname> dir flash:/diagfile/
Directory of flash:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看成员设备的 diagfile 日志：（集中式 IRF 设备）

```
<Sysname> dir slot2#flash:/diagfile/
Directory of slot2#flash:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看设备主用主控板的 diagfile 日志：（分布式设备－独立运行模式）

```
<Sysname> dir cfa0:/diagfile/
Directory of cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看设备备用主控板的 diagfile 日志：（分布式设备－独立运行模式）

```
<Sysname> dir slot1#cfa0:/diagfile/
Directory of slot1#cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看主设备主用主控板的 diagfile 日志：（分布式设备－IRF 模式）

```
<Sysname> dir cfa0:/diagfile/
Directory of cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看主设备备用主控板的 diagfile 日志：（分布式设备－IRF 模式）

```
<Sysname> dir slot1#cfa0:/diagfile/
Directory of slot1#cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

- 查看成员设备主控板的 diagfile 日志，如果成员设备有两块主控板，则两块都需要检查：（分布式设备－IRF 模式）

```
<Sysname> dir chassis2#slot0#cfa0:/diagfile/
Directory of chassis2#slot0#cfa0:/diagfile
   0 -rw-      161321 Jul 11 2013 16:16:00   diagfile18.log

1021104 KB total (421416 KB free)
```

(3) 使用 FTP、TFTP 或者 USB 接口将诊断日志文件传输到指定位置。

1.2.4 诊断信息

诊断信息可以通过两种方式收集：将诊断信息保存到文件，或者将诊断信息直接显示在屏幕上。为保证信息收集的完整性，建议您使用将诊断信息保存到文件的方式收集诊断信息。

需要注意的是，设备上单板越多，诊断信息收集的时间越长，信息收集期间不能输入命令，请耐心等待。

说明

通过 Console 口收集诊断信息所用的时间比通过业务网口收集所用的时间要长。在有可用业务网口或管理口的情况下，建议通过业务网口或管理口登录和传输文件。

(1) 执行 **screen-length disable** 命令，以避免屏幕输出被打断（如果是将诊断信息保存到文件中，则忽略此步骤）。

```
<Sysname>  screen-length disable
```

(2) 执行 **display diagnostic-information** 命令收集诊断信息。

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N] :
```

(3) 选择将诊断信息保存至文件中，还是将直接在屏幕上显示

- 输入“Y”，以及保存诊断信息的路径和名称，将诊断信息保存至文件中。

```
Save or display diagnostic information (Y=save, N=display)? [Y/N] : Y
Please input the file name(*.tar.gz)[ cfa0:/diag.tar.gz] :cfa0:/diag.tar.gz
Diagnostic information is outputting to cfa0:/diag.tar.gz.
Please wait...
Save successfully.
<Sysname> dir cfa0:/
Directory of cfa0:
……
   6 -rw-      898180 Jun 26 2013 09:23:51   diag.tar.gz

1021808 KB total (259072 KB free)
```

- 输入“N”，将诊断信息直接显示在屏幕上。

```
Save or display diagnostic information (Y=save, N=display)? [Y/N] :N
==============================================================
  ===============display alarm===============
No alarm information.
==============================================================
  ===============display boot-loader===============
Software images on slot 0:
Current software images:
  cfa0:/MSR-CMW710-BOOT-R7328_mrpnc.bin
  cfa0:/MSR-CMW710-SYSTEM-R7328_mrpnc.bin
Main startup software images:
  cfa0:/MSR-CMW710-BOOT-R7328_mrpnc.bin
  cfa0:/MSR-CMW710-SYSTEM-R7328_mrpnc.bin
Backup startup software images:
  None
==============================================================
  ===============display counters inbound interface===============
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
BAGG1                        0                  0                  0           0
GE4/0/1                      0                  0                  0           0
GE4/0/2                      2                  2                  0           0
```

GE4/0/3	0	0	0	0
GE4/0/4	0	0	0	0
GE4/0/5	0	0	0	0
GE4/0/6	0	0	0	0
GE4/0/7	0	0	0	0
GE4/0/8	0	0	0	0
GE4/0/9	0	0	0	0
GE4/0/10	0	0	0	0

……

1.3 故障处理求助方式

当故障无法自行解决时，请准备好设备运行信息、故障现象等材料，发送给 H3C 技术支持人员进行故障定位分析。

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

2 硬件类故障处理

2.1 系统类故障

2.1.1 终端无显示或显示乱码

1. 故障描述

设备上电启动时，配置终端无显示或显示乱码。

2. 常见原因

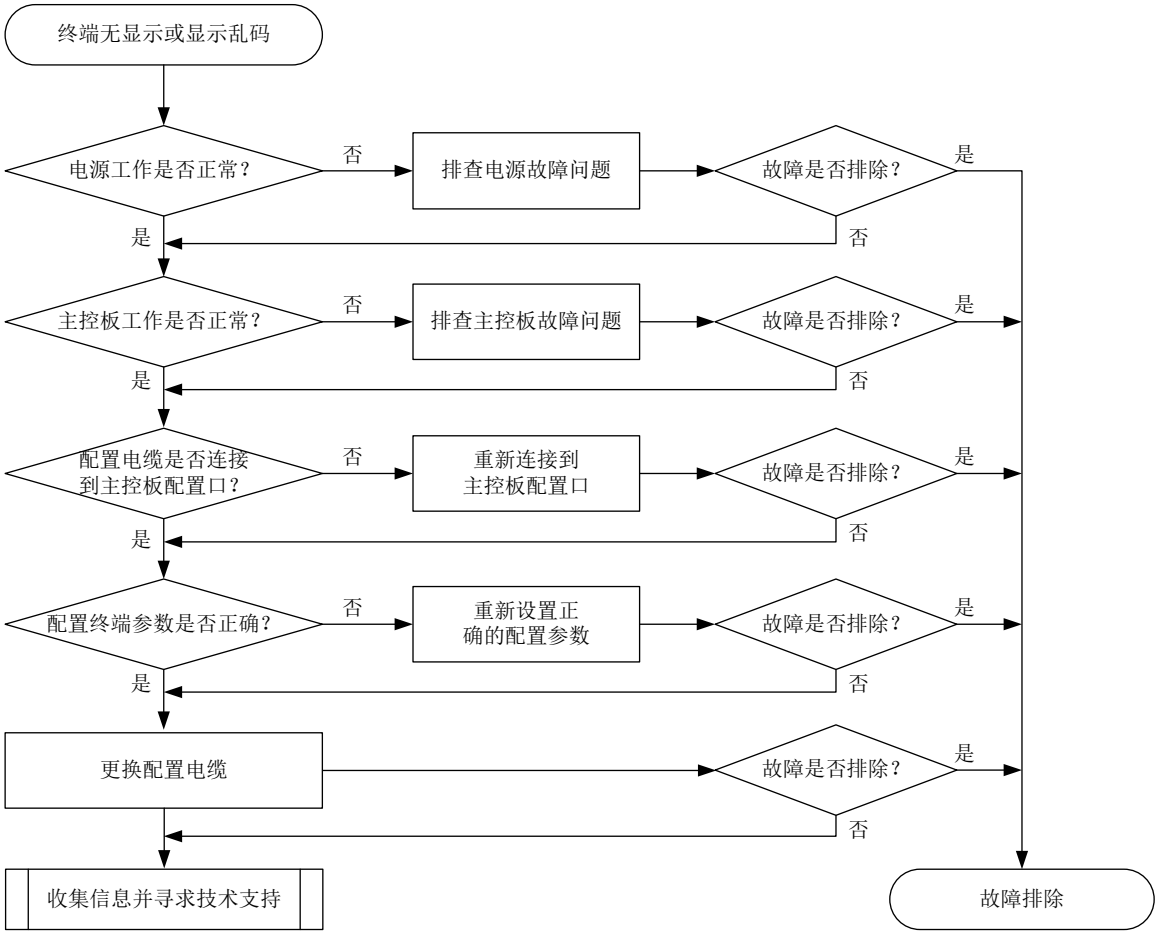
本类故障的常见原因主要包括：

- 电源工作异常。
- 主控板工作异常。
- 配置电缆未连接到主控板的配置口。
- 配置终端参数设置错误。
- 配置电缆故障。

3. 故障分析

本类故障的诊断流程如图 1 所示：

图1 故障诊断流程图



4. 处理步骤

(1) 检查电源工作是否正常。

如果电源模块指示灯状态异常，请参考电源故障处理章节进行处理。

(2) 检查主控板工作是否正常。

如果主控板指示灯状态异常，请参考主控板故障处理章节进行处理。

(3) 检查配置电缆是否已经连接到主控板的配置口。

(4) 检查配置终端 COM 口连接是否正确，实际选择的串口与终端设置的串口要一致，串口参数设置是否正确。

串口参数如下：波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，选择终端仿真为 VT100。不同设备配置的串口参数请以设备实际情况为准。

(5) 更换配置电缆。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

2.1.2 设备异常重启

1. 故障描述

设备在运行中发生异常重启。

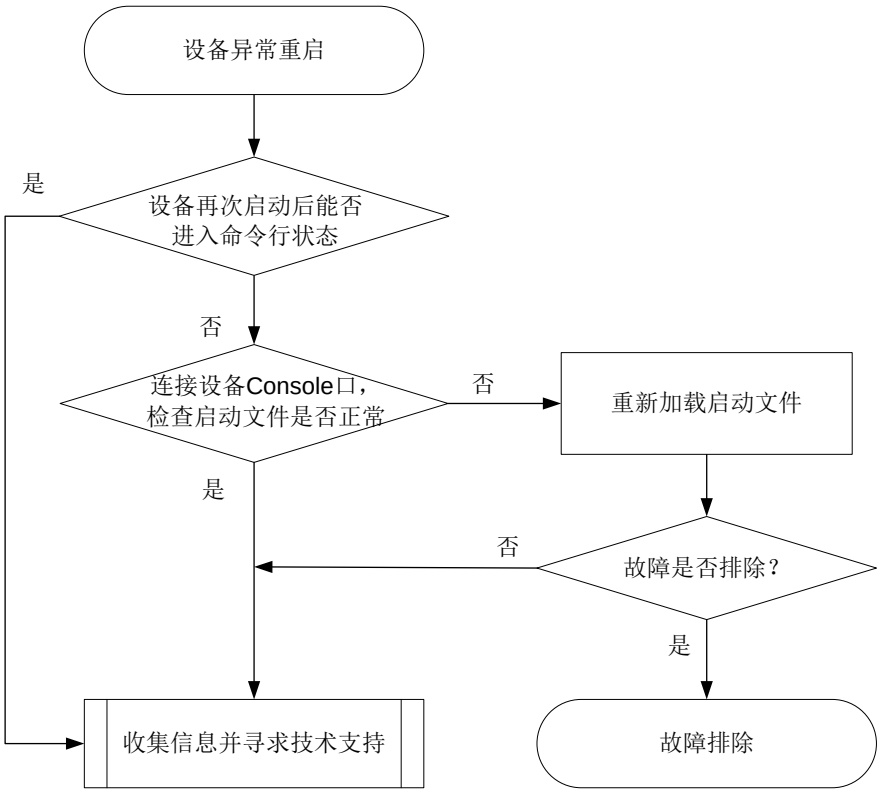
2. 常见原因

本类故障的常见原因启动文件故障。

3. 故障分析

本类故障的诊断流程如图 2 所示：

图2 设备异常重启故障诊断流程图



4. 处理步骤

(1) 查看设备重启后能否进入命令行状态

若设备能够进入命令行状态，请使用 **display diagnostic-information** 命令收集设备的诊断信息，待收集完成后，将设备信息导出后发给 H3C 技术人员支持寻求支持。

说明

执行 **display diagnostic-information** 命令时，可指定 **key-info** 参数仅收集关键诊断信息，从而减少收集时间。

(2) 检查启动文件是否正常

若设备无法进入命令行状态，请通过 Console 口连接设备后再次重启设备，如果 BootWare 提示 CRC 错误或者找不到启动文件，请使用 BootWare 菜单重新下载启动文件，并设置该文件为当前启动文件（在 BootWare 加载过程中，BootWare 能自动将该文件设置为当前启动文件）。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

2.1.3 温度异常告警

1. 故障描述

系统出现温度告警，打印温度过高等告警信息，例如：

```
%Jun 26 10:13:46:233 2013 H3C DRVPLAT/4/DrvDebug: Temperature of the board is too high!
```

2. 常见原因

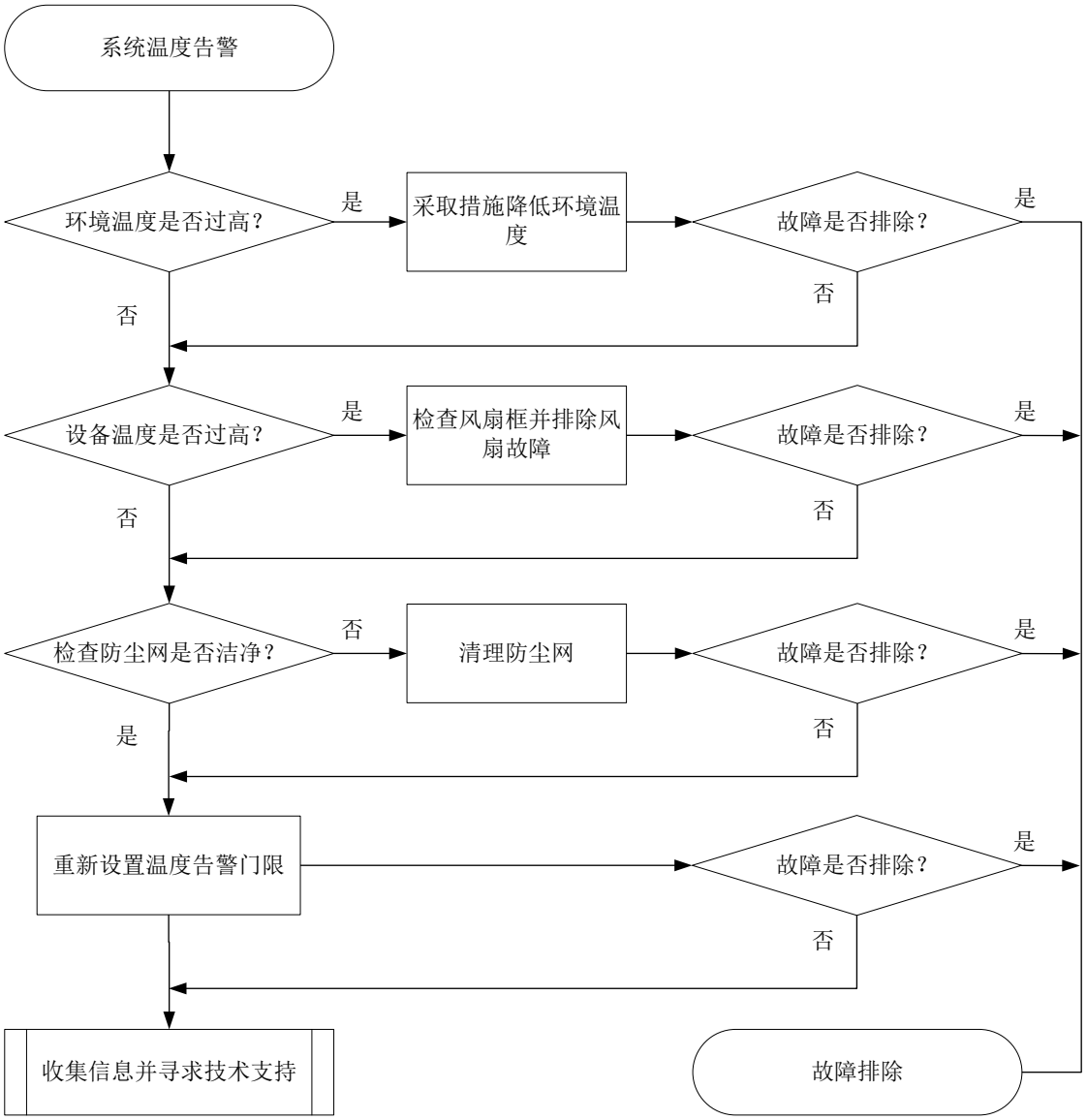
本类故障的常见原因主要包括：

- 机房通风不畅或空调制冷故障等造成环境温度过高。
- 设备风扇故障或出入风口被异物堵塞。
- 设备防尘网积灰过多。
- 温度告警门限设置过低。
- 软件获取温度数据失败，错误告警。

3. 故障分析

本类故障的诊断流程如图 3 所示：

图3 温度异常故障诊断流程图



4. 处理步骤

(1) 检查环境温度是否过高

如果温度过高，请增加空调或者采取其他散热措施降低环境温度。

(2) 检查设备温度是否过高

执行 **display environment** 命令查看设备当前温度值。若显示为 255，则表示软件获取温度数据失败。可多次执行 **display environment** 命令至温度数据正常显示后，判断设备温度是否过高。

若是设备温度过高（设备温度超过一般级高温告警门限），确认设备风扇是否正常并检查出入风口是否被异物堵塞。

使用 **display fan** 命令查看风扇框是否运行正常。若不正常，请参见风扇模块故障章节排除风扇故障。

(3) 检查防尘网是否洁净

如果风扇正常，则检查防尘网是否洁净。清理防尘网后，看温度是否能恢复正常。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

- TEMP_HIGH
- TEMP_LOW
- TEMP_NORMAL
- TEMPERATURE_ALARM
- TEMPERATURE_LOW
- TEMPERATURE_NORMAL
- TEMPERATURE_POWEROFF
- TEMPERATURE_SHUTDOWN
- TEMPERATURE_WARNING

2.1.4 电压异常告警

1. 故障描述

系统打印电压异常告警信息，例如：

```
DEV/4/VOLTAGE_HIGH: Voltage is greater than the high-voltage alarm threshold on chasiss 1 slot 16 voltage sensor 1.
DEV/4/VOLTAGE_LOW: Voltage is less than the low-voltage alarm threshold on chasiss 1 slot 16 voltage sensor 24.
```

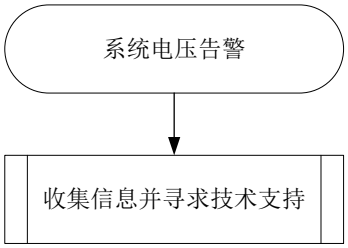
2. 常见原因

本类故障的常见原因一般为硬件出现故障。

3. 故障分析

本类故障的诊断流程如图 4 所示：

图4 电压异常故障诊断流程图



4. 处理步骤

使用 **display voltage** 命令查看设备上电压传感器的电压信息，如果存在异常，请联系技术支持人员。

5. 告警与日志

相关告警

无。

相关日志

- VOLT_HIGH
- VOLT_LOW
- VOLT_NORMAL

2.1.5 内存异常告警

1. 故障描述

系统打印内存异常告警信息，例如：

```
DIAG/1/MEM_EXCEED_THRESHOLD: Memory minor threshold has been exceeded.
```

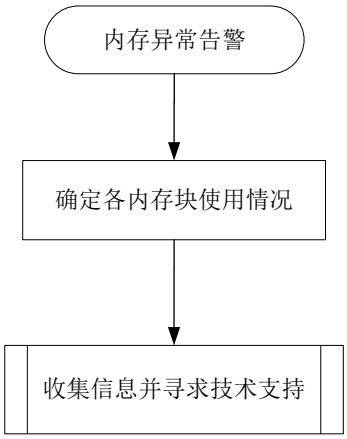
2. 常见原因

本类故障的常见原因主要是由于内存泄露。

3. 故障分析

本类故障的诊断流程如图 5 所示：

图5 内存占用率高故障诊断流程图



4. 处理步骤

(1) 确定各内存块使用情况

通过 Probe 视图下的 **display system internal kernel memory pool** 命令查看各块内存使用情况，找出使用率不正常和不断增加的内存模块。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe] display system internal kernel memory pool slot 1
```

```
Active    Number  Size     Align Slab Pg/Slab ASlabs  NSlabs Name
9126      9248    64       8     32   1       289     289    kmalloc-64
105       112     16328    0     2    8       54      56     kmalloc-16328
14        14      2097096  0     1    512     14      14     kmalloc-2097096
147       225     2048     8     15   8       12      15     kmalloc-2048
7108      7232    192      8     32   2       226     226    kmalloc-192
22        22      524232   0     1    128     22      22     kmalloc-524232
1288      1344    128      8     21   1       64      64     kmalloc-128
0         0       67108808 0     1    16384   0       0      kmalloc-67108808
630       651     4096     8     7    8       93      93     kmalloc-4096
68        70      131016   0     1    32      68      70     kmalloc-131016
1718      2048    8        8     64   1       31      32     kmalloc-8
1         1       16777160 0     1    4096    1       1      kmalloc-16777160
2         15      2048     0     15   8       1       1      sgpool-64
0         0       40       0     42   1       0       0      inotify_event_cache
325       330     16328    8     2    8       165     165    kmalloc_dma-16328
0         0       72       0     30   1       0       0      LFIB_IlmEntryCache
0         0       1080     0     28   8       0       0      LFIB_IlmEntryCache
0         0       1464     0     21   8       0       0      MFW_FsCache
1         20      136      0     20   1       1       1      L2VFIB_Ac_cache
0         0       240      0     25   2       0       0      CCF_JOBDESC
0         0       88       0     26   1       0       0      NS4_Aggre_TosSrcPre
0         0       128      0     21   1       0       0      IPFS_CacheHash_cachep
---- More ----
```

请重点查看 Number 列和 Size 列的统计结果。如果发现某块内存在不停增加，那么表示该块内存在被不断使用。需要注意的是：

- 有些内存块使用率的增加是正常的，所以需要判断该块内存是否真正的异常。Number*Size 是某个模块使用的内存大小。判断内存使用率是否正常可能需要持续观察内存增长速度和内存使用的多少综合分析判断。
- 有些内存的泄漏过程比较缓慢，所以需要比较长的时间（甚至是几周的时间）来对比观察。

(2) 收集信息并寻求技术支持

通过上述步骤只是确定了问题的范围，但还需继续收集信息以确定具体的故障。由于后续信息收集要求较高，不建议用户操作，请与 H3C 的技术支持工程师联系。

需要注意的是，请不要重启设备，否则会将故障信息破坏，给故障定位带来困难。

5. 告警与日志

相关告警

无。

相关日志

- MEM_ALERT
- MEM_EXCEED_THRESHOLD
- MEM_BELOW_THRESHOLD

2.1.6 CPU 占用率高

1. 故障描述

连续使用命令 **display cpu-usage** 查看 CPU 的占用率。如果 CPU 占用率持续在 80%以上，说明有某个任务长时间占用 CPU，需要确认 CPU 高的具体原因。

```
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      80% in last 5 seconds
      80% in last 1 minute
      80% in last 5 minutes
```

2. 常见原因

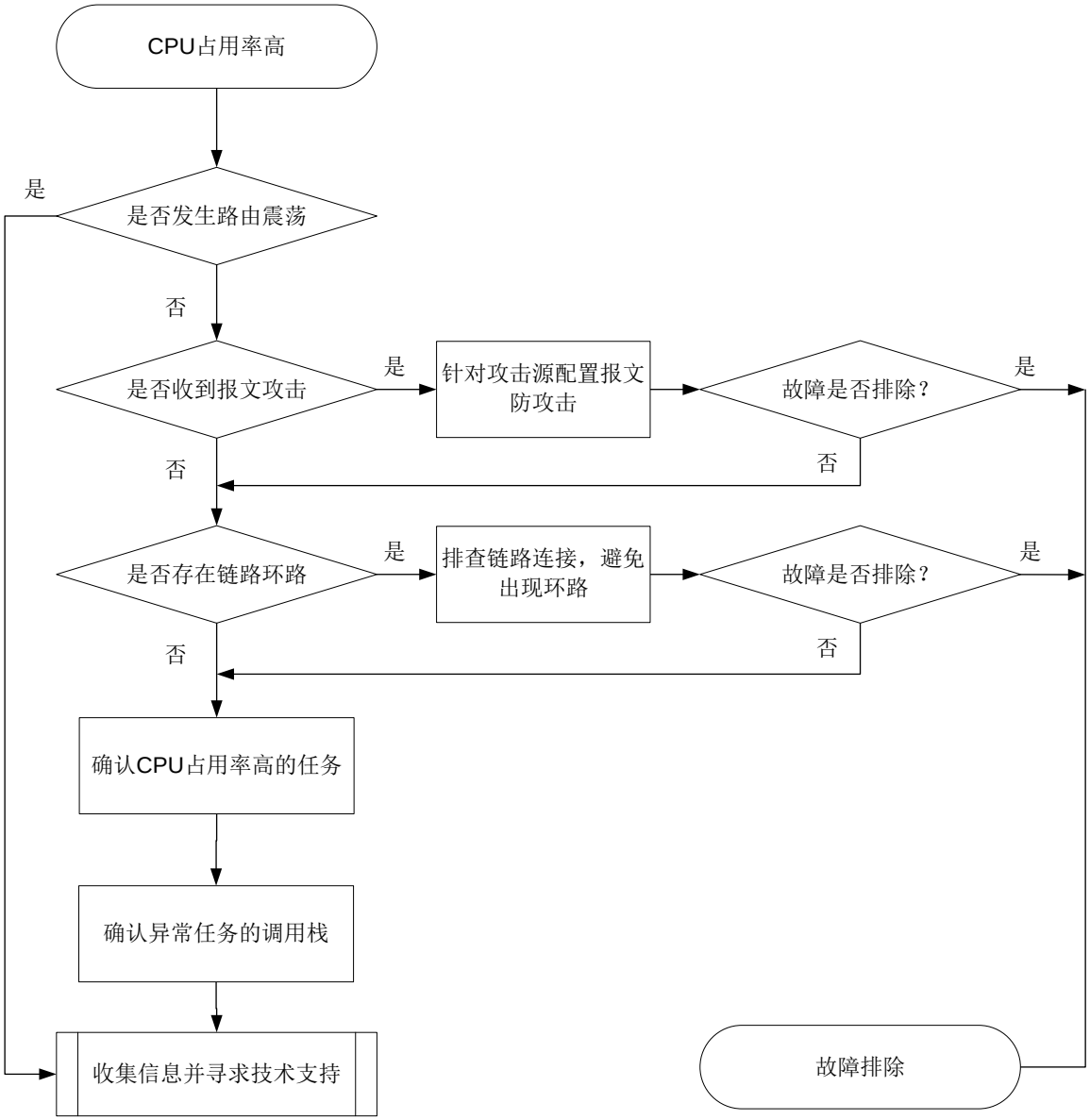
本类故障的常见原因主要包括：

- 路由振荡
- 报文攻击
- 链路环路

3. 故障分析

本类故障的诊断流程如图 6 所示：

图6 CPU 占用率高故障诊断流程图



4. 处理步骤

(1) 检查是否发生路由振荡

路由表中条目频繁变化，可能导致 CPU 占用率过高。当发生路由震荡时，请收集信息并联系 H3C 技术人员寻求技术支持。

首次查看路由表：

```
[Sysname] display ip routing-table

         Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
```

```
10.1.1.0/24          OSPF   150  1            11.2.1.1        Vlan100
127.0.0.0/8          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32         Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32   Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4          Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24         Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32   Direct 0    0            127.0.0.1       InLoop0
```

再次查看路由表：

```
[Sysname] display ip routing-table

         Destinations : 8        Routes : 8

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

(2) 检查是否受到报文攻击

通过抓包确认攻击源。在设备端口抓包，使用报文捕获工具（如 Sniffer、Wireshark、WinNetCap 等）分析报文特征，确认攻击源。然后针对攻击源配置报文防攻击。关于报文防攻击的详细介绍和配置，请参见“安全配置指导”中的“攻击检测与防范”。

(3) 检查是否存在链路

链路存在环路时，可能出现广播风暴和网络振荡，大量的协议报文上送 CPU 处理可能导致 CPU 占用率升高，设备很多端口的流量会变得很大，端口使用率达到 90%以上：

```
<Sysname> display interface gigabitethernet3/0/1
GigabitEthernet3/0/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet3/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet address: 2.1.1.2/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0000-fc00-9276
IPv6 packet frame type: Ethernet II, hardware address: 0000-fc00-9276
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T
Port priority: 0
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
```

```
Last clearing of counters: Never
 Peak input rate: 8 bytes/sec, at 2016-03-19 09:20:48
 Peak output rate: 1 bytes/sec, at 2016-03-19 09:16:16
 Last 300 second input: 26560 packets/sec 123241940 bytes/sec 99%
 Last 300 second output: 0 packets/sec 0 bytes/sec 0%
……
```

如链路出现环路：

- 排查链路连接、端口配置是否正确。
- 对于二层口，是否使能 STP 协议，配置是否正确。
- 对于二层口，邻接设备 STP 状态是否正常。
- 如以上配置均正确，可能为 STP 协议计算错误或协议计算正确但端口驱动层没有正常 Block 阻塞，可以 shutdown 环路上端口、拔插端口让 STP 重新计算来快速恢复业务。

(4) 确定 CPU 占用率高的任务

如果通过上述步骤无法解决故障，请通过 **display process cpu** 命令观察占用 CPU 最多的任务。

```
<Sysname> display process cpu slot 1
CPU utilization in 5 secs: 2.4%; 1 min: 2.5%; 5 mins: 2.4%
    JID      5Sec      1Min      5Min    Name
      1      0.0%      0.0%      0.0%    scmd
      2      0.0%      0.0%      0.0%    [kthreadd]
      3      0.0%      0.0%      0.0%    [migration/0]
      4      0.0%      0.0%      0.0%    [ksoftirqd/0]
      5      0.0%      0.0%      0.0%    [watchdog/0]
      6      0.0%      0.0%      0.0%    [migration/1]
      7      0.0%      0.0%      0.0%    [ksoftirqd/1]
      8      0.0%      0.0%      0.0%    [watchdog/1]
      9      0.0%      0.0%      0.0%    [migration/2]
     10      0.0%      0.0%      0.0%    [ksoftirqd/2]
     11      0.0%      0.0%      0.0%    [watchdog/2]
……
```

各列分别表示某任务平均 5sec、1min、5min 占用 CPU 的百分比和任务名。某任务占用率越高，说明相应的任务占用 CPU 的资源越多。正常情况任务对 CPU 的占用率一般低于 5%，这个命令可以查看明显高出正常占用率的任务。

(5) 确认异常任务的调用栈

通过 Probe 视图下的 **follow job** *job-id* 命令确认异常任务的调用栈，请查询 5 次以上，发送给技术支持人员分析，以便于分析该任务具体在做什么处理导致 CPU 占用率持续升高。此处以显示 JID 145 的调用栈为例。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe] follow job 145 slot 1
Attaching to process 145 ([dGDB])
Iteration 1 of 5
------------------------------
Kernel stack:
[<ffffffff80355290>] schedule+0x570/0xde0
```

```
[<ffffffff80355da8>] schedule_timeout+0x98/0xe0
[<ffffffff802047e4>] ep_poll+0x4b4/0x5e0
[<ffffffffc05587a8>] DRV_Sal_EVENT_Read+0x1f8/0x290 [system]
[<ffffffffc07351e4>] drv_sysm_gdb_console+0xc4/0x2d0 [system]
[<ffffffffc1a04114>] thread_boot+0x84/0xa0 [system]
[<ffffffff8015c420>] kthread+0x130/0x140
[<ffffffff801183d0>] kernel_thread_helper+0x10/0x20

Iteration 2 of 5
------------------------------
Kernel stack:
[<ffffffff80355290>] schedule+0x570/0xde0
[<ffffffff80355da8>] schedule_timeout+0x98/0xe0
[<ffffffff802047e4>] ep_poll+0x4b4/0x5e0
[<ffffffffc05587a8>] DRV_Sal_EVENT_Read+0x1f8/0x290 [system]
[<ffffffffc07351e4>] drv_sysm_gdb_console+0xc4/0x2d0 [system]
[<ffffffffc1a04114>] thread_boot+0x84/0xa0 [system]
[<ffffffff8015c420>] kthread+0x130/0x140
[<ffffffff801183d0>] kernel_thread_helper+0x10/0x20

Iteration 3 of 5
------------------------------
Kernel stack:
[<ffffffff80355290>] schedule+0x570/0xde0
[<ffffffff80355da8>] schedule_timeout+0x98/0xe0
[<ffffffff802047e4>] ep_poll+0x4b4/0x5e0
[<ffffffffc05587a8>] DRV_Sal_EVENT_Read+0x1f8/0x290 [system]
[<ffffffffc07351e4>] drv_sysm_gdb_console+0xc4/0x2d0 [system]
[<ffffffffc1a04114>] thread_boot+0x84/0xa0 [system]
[<ffffffff8015c420>] kthread+0x130/0x140
[<ffffffff801183d0>] kernel_thread_helper+0x10/0x20

Iteration 4 of 5
------------------------------
Kernel stack:
[<ffffffff80355290>] schedule+0x570/0xde0
[<ffffffff80355da8>] schedule_timeout+0x98/0xe0
[<ffffffff802047e4>] ep_poll+0x4b4/0x5e0
[<ffffffffc05587a8>] DRV_Sal_EVENT_Read+0x1f8/0x290 [system]
[<ffffffffc07351e4>] drv_sysm_gdb_console+0xc4/0x2d0 [system]
[<ffffffffc1a04114>] thread_boot+0x84/0xa0 [system]
[<ffffffff8015c420>] kthread+0x130/0x140
[<ffffffff801183d0>] kernel_thread_helper+0x10/0x20

Iteration 5 of 5
------------------------------
Kernel stack:
[<ffffffff80355290>] schedule+0x570/0xde0
```

```
[<ffffffff80355da8>] schedule_timeout+0x98/0xe0
[<ffffffff802047e4>] ep_poll+0x4b4/0x5e0
[<ffffffffc05587a8>] DRV_Sal_EVENT_Read+0x1f8/0x290 [system]
[<ffffffffc07351e4>] drv_sysm_gdb_console+0xc4/0x2d0 [system]
[<ffffffffc1a04114>] thread_boot+0x84/0xa0 [system]
[<ffffffff8015c420>] kthread+0x130/0x140
[<ffffffff801183d0>] kernel_thread_helper+0x10/0x20
```

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

- CPU_STATE_NORMAL
- CPU_MINOR_RECOVERY
- CPU_MINOR_THRESHOLD
- CPU_SEVERE_RECOVERY
- CPU_SEVERE_THRESHOLD

2.2 电源类故障

2.2.1 电源模块状态异常

1. 故障描述

电源模块状态指示灯异常或者电源运行中上报 Fault。

2. 常见原因

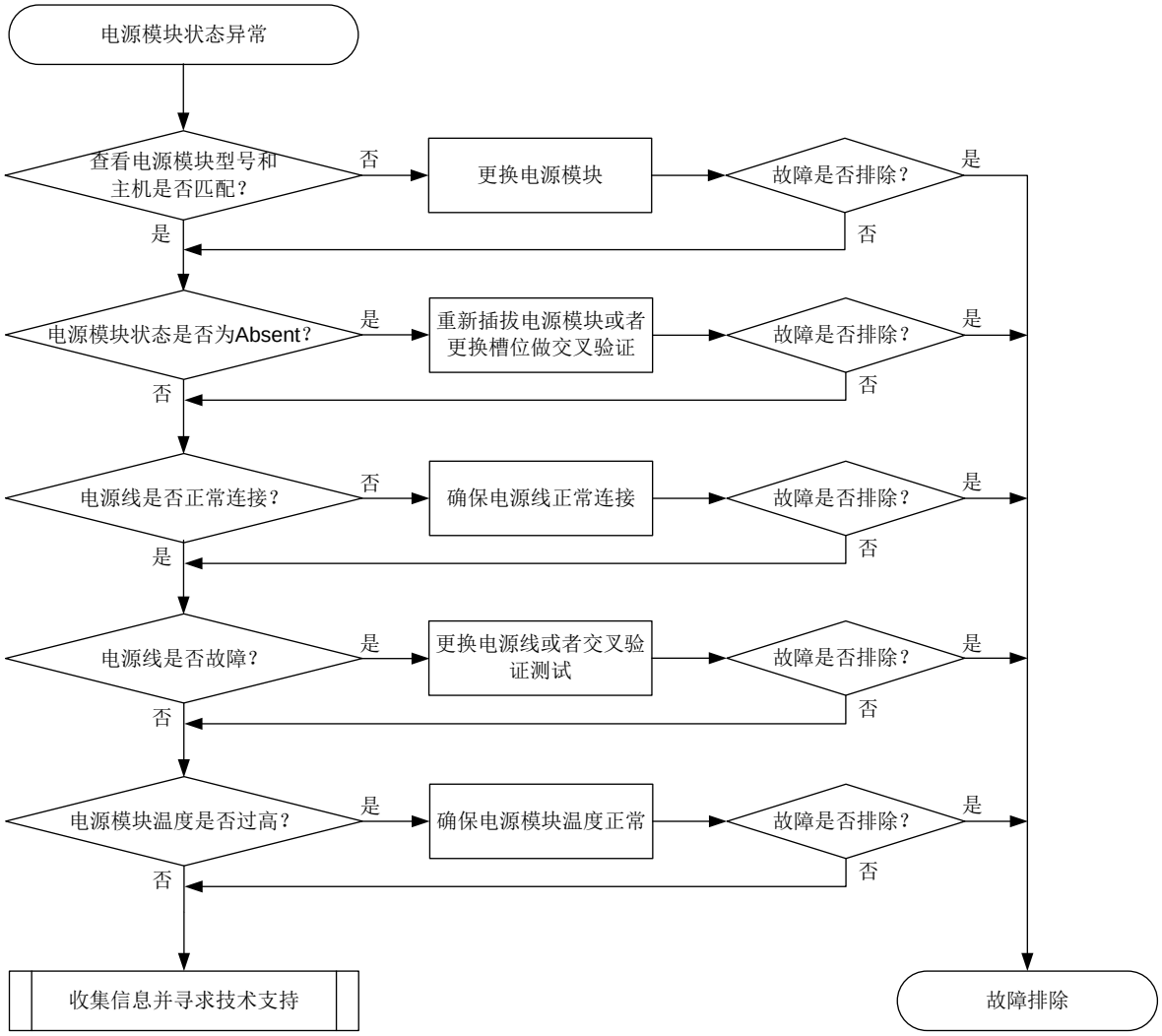
本类故障的常见原因主要包括：

- 电源模块型号和主机不匹配。
- 电源模块安装不到位。
- 电源线缆没有插牢。
- 电源模块温度过高。
- 电源模块故障。

3. 故障分析

本类故障的诊断流程如图 7 所示。

图7 故障诊断流程图



4. 处理步骤

(1) 检查电源模块的型号是否和主机型号匹配。

(2) 检查设备连接的供电系统：确认供电系统正常供电，电压正常。

(3) 检查电源模块状态。

使用 **display power** 命令显示电源模块状态，查看是否存在 Fail 或 Absent 状态的电源模块。

```
<Sysname> display power
 Index         Status
 ----------------------
 PWR1          normal
 PWR2          Absent
```

也可以使用 **display alarm** 命令查看电源模块告警信息。

```
<Sysname> display alarm
Slot   CPU   Level   Info
-      -     INFO    Power 1 is absent.
```

```
-       -       INFO    Power 2 is absent.
-       -       INFO    Power 3 is absent.
```

(4) 如果电源模块状态为 Absent，请按如下子步骤进行定位处理。

a. 请将该电源模块拆卸后重新安装，重新安装前请检查电源连接器是否完好。

b. 重新安装后，该电源模块的状态未恢复为 Normal，则请将该电源模块与正常的电源模块更换槽位再做一次交叉验证。

c. 如果该电源模块仍然显示为 Absent，则请更换新的电源模块。

d. 更换新的电源模块后，此故障仍然存在，请执行步骤 7。

(5) 如果电源模块状态为 Fail，请按如下子步骤进行定位处理。

a. 检查电源线是否脱落或者是否正确连接。

b. 如果电源线连接正常，交叉验证下电源线是否故障。

c. 如果电源线正常，可能是电源模块本身温度过高导致。请查看电源模块积灰情况，如果灰尘较多，请清理灰尘，并将电源模块拆卸后重新安装。

d. 重新安装后，电源模块状态未恢复为 Normal，请将该电源模块与正常的电源模块更换槽位做一次交叉验证。

e. 如果该电源模块仍然显示为 Fail 状态，请更换电源模块。

f. 更换新电源模块后，此故障仍然存在，请执行步骤 7。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- DEV/2/POWER_FAILED
- DEV/3/POWER_ABSENT

2.3 单板故障

2.3.1 单板状态异常故障

1. 故障描述

- 单板状态异常（比如执行 display device 命令查看单板状态为 Absent、Fault 等）。
- 单板出现异常重启、无法启动或不断重启等。

2. 常见原因

本类故障的常见原因主要包括：

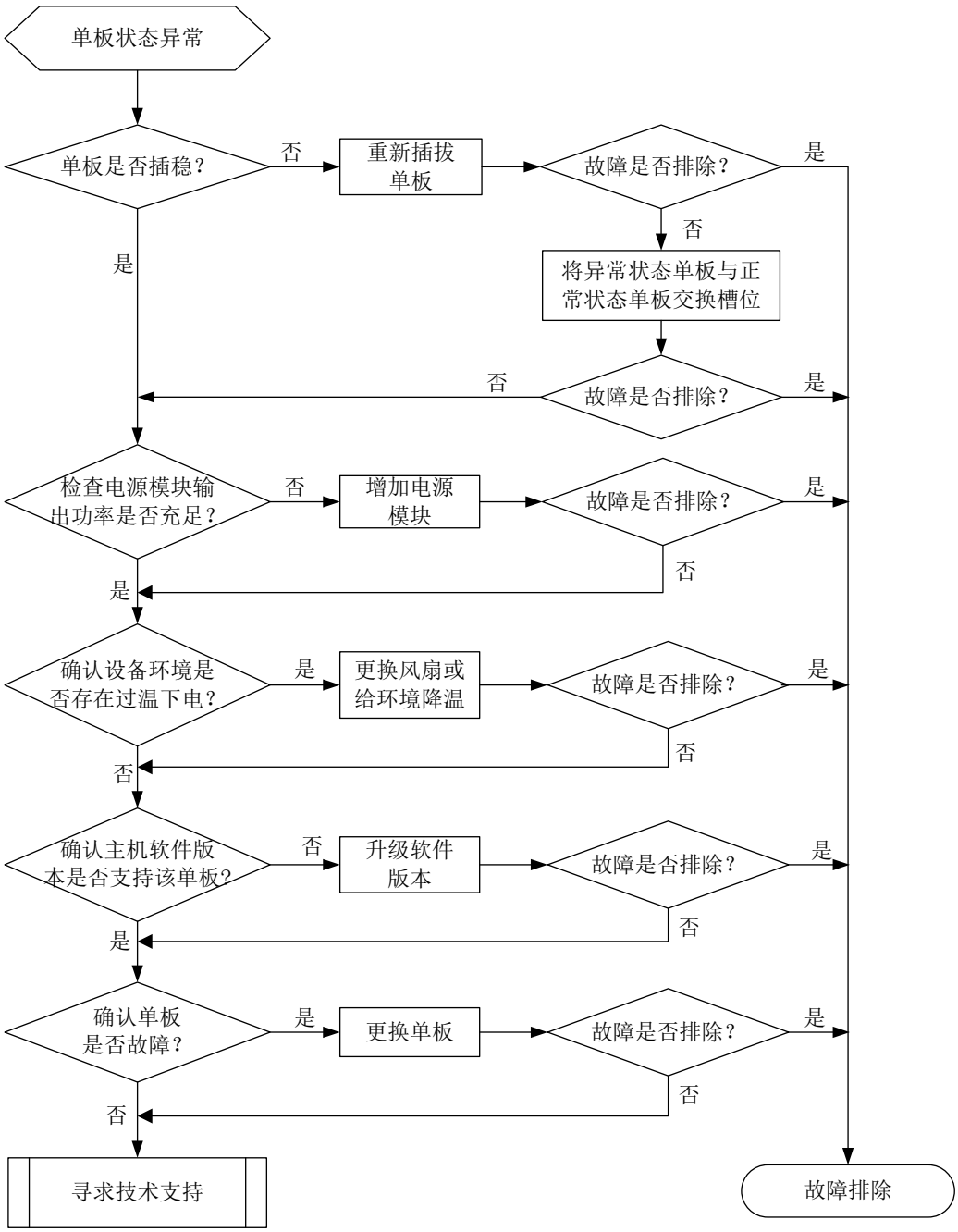
- 单板安装不到位。
- 单板损坏。
- 单板面板的指示灯点亮异常。

- 电源模块故障。
- 电源模块输出功率不足。
- 主机软件版本不支持使用该单板。

3. 故障分析

本类故障的诊断流程如图 8 所示。

图8 单板状态异常故障诊断流程图



4. 处理步骤

- 单板状态 Absent

(1) 确认单板是否插稳，如检查单板与机框之间是否有空隙，也可以将单板拔出后重插入。重新插入前务必检查单板的连接器状态，看连接器是否变形、脏污。

(2) 将单板放到别的槽位，将框上别的正常的单板放到这个槽位，进一步确认是不是单板故障。

(3) 检查单板面板的指示灯是否点亮。

(4) 确认电源模块输出功率是否充足。比如增加电源模块，看该单板状态是否恢复正常。

(5) 确认主机软件版本是否支持该单板。

a. 通过 **display version** 命令查看主机软件版本；

b. 联系技术支持，确认当前主机软件版本是否支持该单板；

c. 如果当前软件版本不支持该单板，请升级到正确版本，版本升级前务必确认新版本可以兼容其它单板。

(6) 如确认为单板故障，请更换单板，收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

- 单板状态 Power-off。

(7) 确认设备环境是否存在过温下电，通过命令 **display power-supply** 查看是否存在环境温度过高，单板被下电的记录。比如单板的供电状态“Status”为“off”表示单板由于用户操作或过温保护等原因被主动下电。

```
<Sysname> display power-supply verbose
Index          Status          Type            Description
  ------------------------------------------------------------
  PWR1           normal          10W DC Power
```

如果确认是过温下电，请排查环境单板槽位是否插满，如果单板槽位已插满单板或者挡风板，请通过命令 **display fan** 确认风扇工作是否正常，风扇状态为 Normal 表示风扇正常工作，如不正常，或确认单板存在电源故障，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

- 单板状态 Fault。

(8) 检查整机功耗，整机功耗不够时，单板会进入 fault 状态。

(9) 等待一段时间（大约 10 分钟左右）确认下单板是一直 Fault 还是 Normal 后又再次重启。如单板是 Normal 后又自动重启，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

(10) 如果单板是主控板，请连上串口线，查看配置终端上是否有单板正常启动的显示信息、或单板启动是否异常。如下述主控板启动时出现内存读写测试失败而不断重启，需要检查主控板内存条是否插稳。

```
readed value is 55555555 , expected value is aaaaaaaa
DRAM test fails at: 080ffff8
DRAM test fails at: 080ffff8
Fatal error! Please reboot the board.
```

(11) 将单板放到别的槽位，进一步确认是不是槽位故障。

(12) 如确认为单板故障，请更换单板，收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

- 单板重启异常

  这里的单板重启是指单板出现过重启，而当前单板状态是 Normal。

(13) 通过日志或运行时间分析重启的时间段，确认重启的时间点附近有无用户通过命令行 **reboot** 重启或进行单板上下电等操作。

(14) display version 命令支持查询单板最近一次重启的原因。比如“Last reboot reason”表示单板最近一次重启原因是设备上电。

```
<Sysname> display version
H3C Comware Software, Version 7.1.064, Release 6728P17
Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.
H3C MSR810 uptime is 0 weeks, 1 day, 19 hours, 11 minutes
Last reboot reason : User reboot
Boot image: flash:/msr810s-cmw710-boot-r6728p17.bin
Boot image version: 7.1.064P80, Release 6728P17
  Compiled Mar 23 2022 15:00:00
System image: flash:/msr810s-cmw710-system-r6728p17.bin
System image version: 7.1.064, Release 6728P17
  Compiled Mar 23 2022 15:00:00
Feature image(s) list:
  flash:/msr810s-cmw710-devkit-r6728p17.bin, version: 7.1.064
    Compiled Mar 23 2022 15:00:00
  flash:/msr810s-cmw710-data-r6728p17.bin, version: 7.1.064
    Compiled Mar 23 2022 15:00:00

CPU ID: 0xa
512M bytes DDR3 SDRAM Memory
256M bytes Flash Memory
PCB               Version:  2.0
CPLD              Version:  0.0
Basic    BootWare Version:  1.11
Extended BootWare Version:  1.11
[SLOT  0]CON                      (Hardware)2.0,   (Driver)1.0,   (CPLD)0.0
[SLOT  0]4FSW                     (Hardware)2.0,   (Driver)1.0,   (CPLD)0.0
[SLOT  0]CELLULAR0/0              (Hardware)2.0,   (Driver)1.0,   (CPLD)0.0
[SLOT  1]CELLULAR                 (Hardware)1.0,   (Driver)1.0,   (CPLD)0.0
```

(15) 如果所有单板同时出现重启，请检查设备电源模块是否正常，确认外部电源是否出现过停电，电源进线是否插稳、是否出现松动。

(16) 如无法确认，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

2.4 端口故障

2.4.1 端口出现 CRC 错误

1. 故障描述

通过 **display interface** 查看到端口存在 CRC 错包。

```
<Sysname> display interface gigabitethernet1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet address: 2.1.1.2/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0000-fc00-9276
IPv6 packet frame type: Ethernet II, hardware address: 0000-fc00-9276
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T
Port priority: 0
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Last clearing of counters: Never
 Peak input rate: 8 bytes/sec, at 2019-03-19 09:20:48
 Peak output rate: 1 bytes/sec, at 2019-03-19 09:16:16
 Last 300 second input: 0 packets/sec 0 bytes/sec -%
 Last 300 second output: 0 packets/sec 0 bytes/sec -%
 Input (total):  2892 packets, 236676 bytes
          24 unicasts, 2 broadcasts, 2866 multicasts, 0 pauses
 Input (normal):  2892 packets, - bytes
          24 unicasts, 2 broadcasts, 2866 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          3 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 29 packets, 1856 bytes
          24 unicasts, 5 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 29 packets, - bytes
          24 unicasts, 5 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

以上显示信息表明，入端口出现了 CRC 错包。

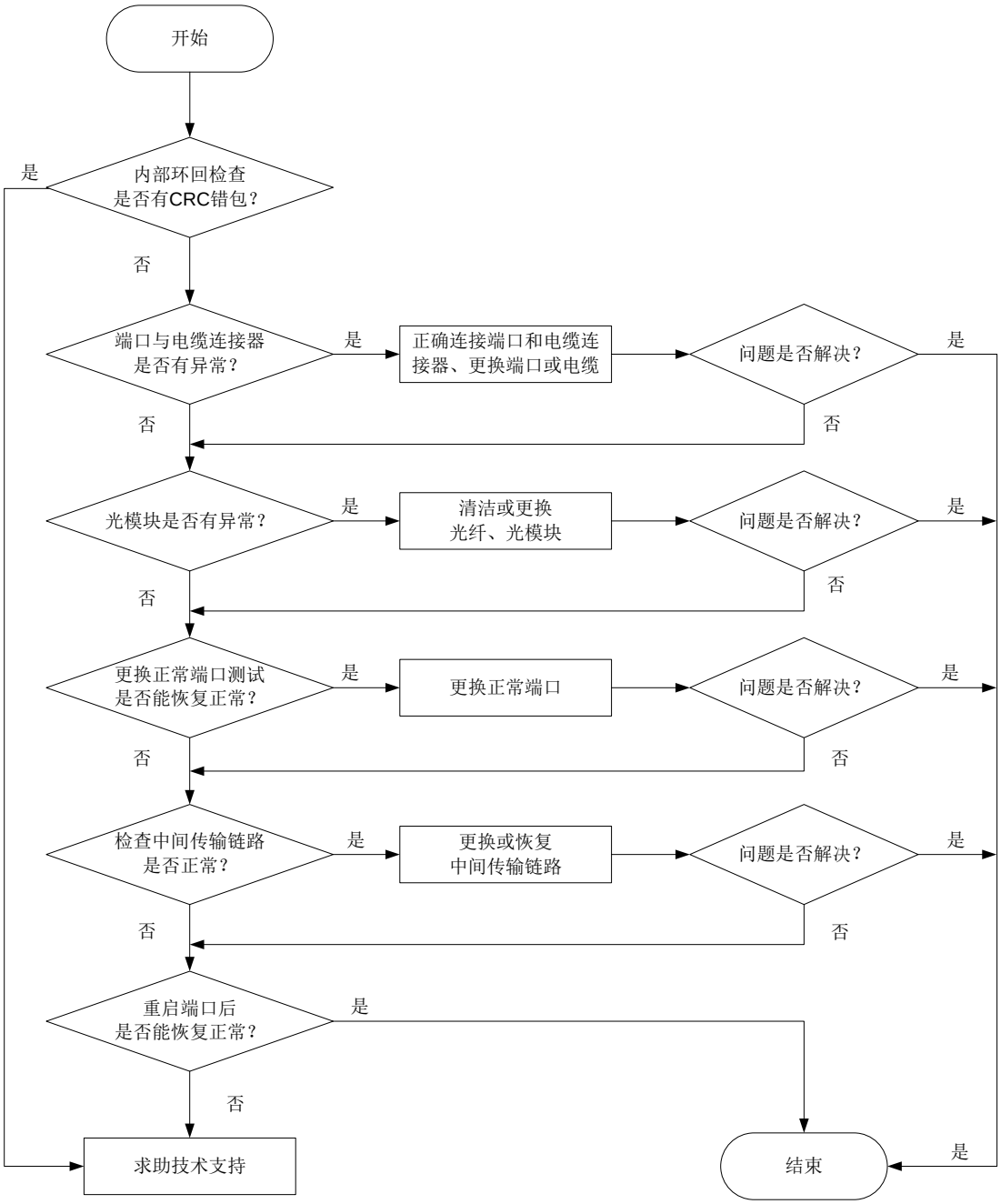
2. 常见原因

- 端口与电缆连接器物理连接有虚插现象。
- 端口异常。
- 电缆连接器损坏。
- 光模块、光纤有污染或连接不好。
- 光功率不足。
- 中间链路或设备故障。
- 设备或单板硬件故障。

3. 故障分析

本类故障的诊断流程如图 9 所示。

图9 故障诊断流程图



4. 处理步骤

(1) 端口进行内部环回检查。

在端口下配置 **loopback internal** 命令开启内部环回功能，然后通过 **display interface** 查看端口 CRC 错包统计是否增长。如果增长，则可能是设备或单板硬件故障，请联系技术支持人员。如果不增长，则不是端口内部问题。

(2) 检查端口与电缆连接器是否有异常。

a. 检查端口和电缆连接器的物理连接是否有虚插。若有虚插，请正确连接端口和电缆连接器。

b. 检查端口是否异常，比如端口内存在异物，端口的 PIN 针有弯针，端口的外壳变形等异常。若有异常，需要更换其他正常端口或光模块。

c. 检查电缆连接器是否出现损坏现象。若有损坏现象，请更换电缆。

(3) 检查光模块是否有异常。

a. 将使用光纤将该端口的光模块 Tx 端和 Rx 端连接，然后通过 **display interface** 查看端口 CRC 错包统计是否增长。如果增长，则可能是光模块的问题。如果不增长，则不是该光模块问题。

b. 通过 **display transceiver alarm** 命令查看光模块是否有 Rx_Los 或 Tx_Fault 告警信息，若有告警信息，需要清洁或更换光纤、光模块。

c. 通过 **display transceiver diagnosis** 命令查看光模块的接收功率和发送功率是否在规定的最大值和最小值的范围内，若有接收或发送的功率超出范围，需要清洁或更换光纤、光模块。

(4) 更换正常端口测试是否能恢复正常。

更换其他正常的端口测试，如果端口更换后错包消失，端口更换回来错包又再次出现，则为端口硬件故障，请更换端口并将故障信息发送技术支持人员分析；如更换到其他正常端口仍会出现错包，则中间传输链路故障的可能性较大。

(5) 检查中间传输链路是否正常。

使用仪器测试中间链路，链路质量差或者线路光信号衰减过大会导致报文在传输过程中出错。检查互连中间链路设备（光转，转接架，传输等设备）是否正常。若中间传输链路故障，请更换或恢复中间传输链路。

(6) 执行 **shutdown** 命令，再执行 **undo shutdown** 命令，查看端口是否能恢复正常。

(7) 如果故障仍然未能排除，可能是设备或单板硬件故障，请收集信息，并联系技术支持人员。

5. 告警与日志

相关告警

无。

相关日志

无。

2.4.2 端口不接收报文

1. 故障描述

端口状态为 UP，不接收报文或出现丢包。

使用 **display interface** 命令查看本端入方向的接收报文统计增长数量小于对端出方向发送报文统计增长数量。

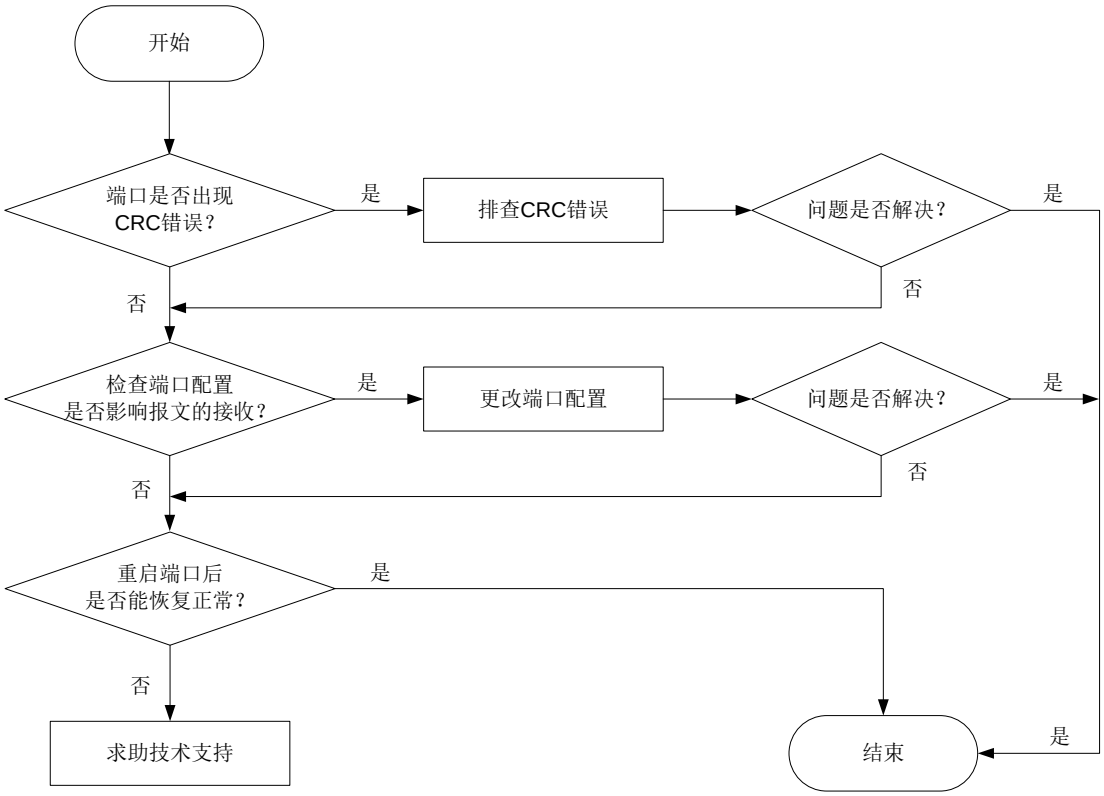
2. 常见原因

- 端口出现 CRC 错误。
- 端口上的配置影响报文的接收。
- 设备或单板硬件故障。

3. 故障分析

本类故障的诊断流程如图 10 所示。

图10 故障诊断流程图



4. 处理步骤

(1) 查看端口是否出现 CRC 错误。

按“端口出现 CRC 错误”章节排查。

(2) 检查端口配置是否影响报文接收。

可通过以下步骤检查端口配置是否影响报文的接收：

- 通过 **display interface brief** 命令，查看端口配置是否有异常。其中包括两端的端口双工模式、端口类型以及 VLAN 等配置。若有异常，请更改端口属性的配置查看该故障端口是否能恢复正常。如果不能，请先执行 **shutdown** 命令后，再执行 **undo shutdown** 命令，再次查看端口是否能恢复正常。
- 对于二层口，如果配置了 STP 功能，通过 **display stp brief** 命令，查看端口是否为 discarding 状态。如果端口被 STP 设置为 discarding 状态，请根据 STP 的相关配置进一步排查。建议将连接终端设备的端口配置为边缘端口或关闭该端口的 STP 功能。
- 如果该端口加入了聚合组，通过 **display link-aggregation summary** 命令查看该端口是否为 Selected 选中状态。当该端口 Status 为 Unselected 状态时，该端口无法收发数据报文。请定位端口成为 Unselected 状态的原因，如聚合组内成员端口的属性类配置与参考端口不一致，进一步排查解决。
- 如果配置了 ACL 过滤，请根据 ACL 的相关配置进一步排查。

- 如果接口上配置了广播/组播/未知单播风暴抑制功能，当接口上的广播/组播/未知单播流量超过用户设置的抑制阈值时，系统会丢弃超出流量限制的报文，查看接口是否配置了了广播/组播/未知单播风暴抑制功能，如果配置了，请关闭接口的风暴抑制功能查看该故障端口是否能恢复正常。

(3) 执行 **shutdown** 命令，再执行 **undo shutdown** 命令，查看端口是否能恢复正常。

(4) 如果故障仍然未能排除，可能是设备或单板硬件故障，请收集信息，并联系技术支持人员。

5. 告警与日志

相关告警

无。

相关日志

无。

2.4.3 端口不发送报文

1. 故障描述

端口状态为 UP，但不发送报文。

使用 **display interface** 命令查看本端出方向的发送报文统计不增长。

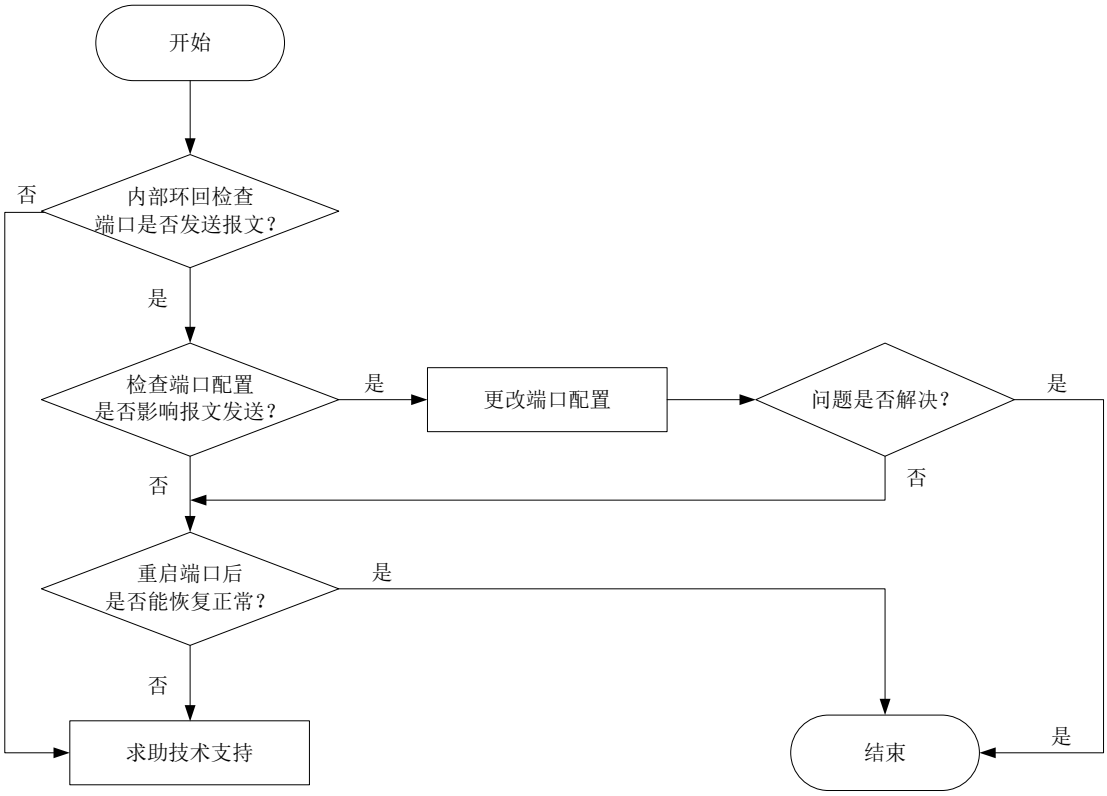
2. 常见原因

- 光模块异常。
- 端口上的配置影响报文的接收。
- 设备或单板硬件故障。

3. 故障分析

本类故障的诊断流程如图 11 所示。

图11 故障诊断流程图



4. 处理步骤

(1) 端口进行内部环回检查。

在端口下配置 **loopback internal** 命令开启内部环回功能，然后通过 **display interface** 查看本端出方向的发送报文统计是否增长。如果不增长，则可能是设备或单板硬件故障，请联系技术支持人员。如果不增长，则不是端口内部问题。

(2) 检查端口配置是否影响报文发送。

可通过以下步骤检查端口配置是否影响报文的发送：

- 对于二层口，如果配置了 STP 功能，通过 **display stp brief** 命令，查看端口是否为 discarding 状态。如果端口被 STP 设置为 discarding 状态，请根据 STP 的相关配置进一步排查。建议将连接终端设备的端口配置为边缘端口或关闭该端口的 STP 功能。
- 如果该端口加入了聚合组，通过 **display link-aggregation summary** 命令查看该端口是否为 Selected 选中状态。当该端口 Status 为 Unselected 状态时，该端口无法收发数据报文。请定位端口成为 Unselected 状态的原因，如聚合组内成员端口的属性类配置与参考端口不一致，进一步排查解决。
- 如果配置了 ACL 过滤，请根据 ACL 的相关配置进一步排查。
- 查看是否配置了接口出方向上阻断广播/未知组播/未知单播报文功能，某些协议（例如 ARP、DHCP、RIP、IGMP 等）在运行过程中会交互广播/未知组播/未知单播报文，如果配置该功能将导致这些协议报文不能通过该接口发送，请关闭该功能查看故障端口是否能恢复正常。

(3) 执行 **shutdown** 命令，再执行 **undo shutdown** 命令，查看端口是否能恢复正常。

(4) 如果故障仍然未能排除，可能是设备或单板硬件故障，请收集信息，并联系技术支持人员。

5. 告警与日志

相关告警

无。

相关日志

无。

2.4.4 电口无法 UP

1. 故障描述

电口连接线缆后无法正常 UP。

2. 常见原因

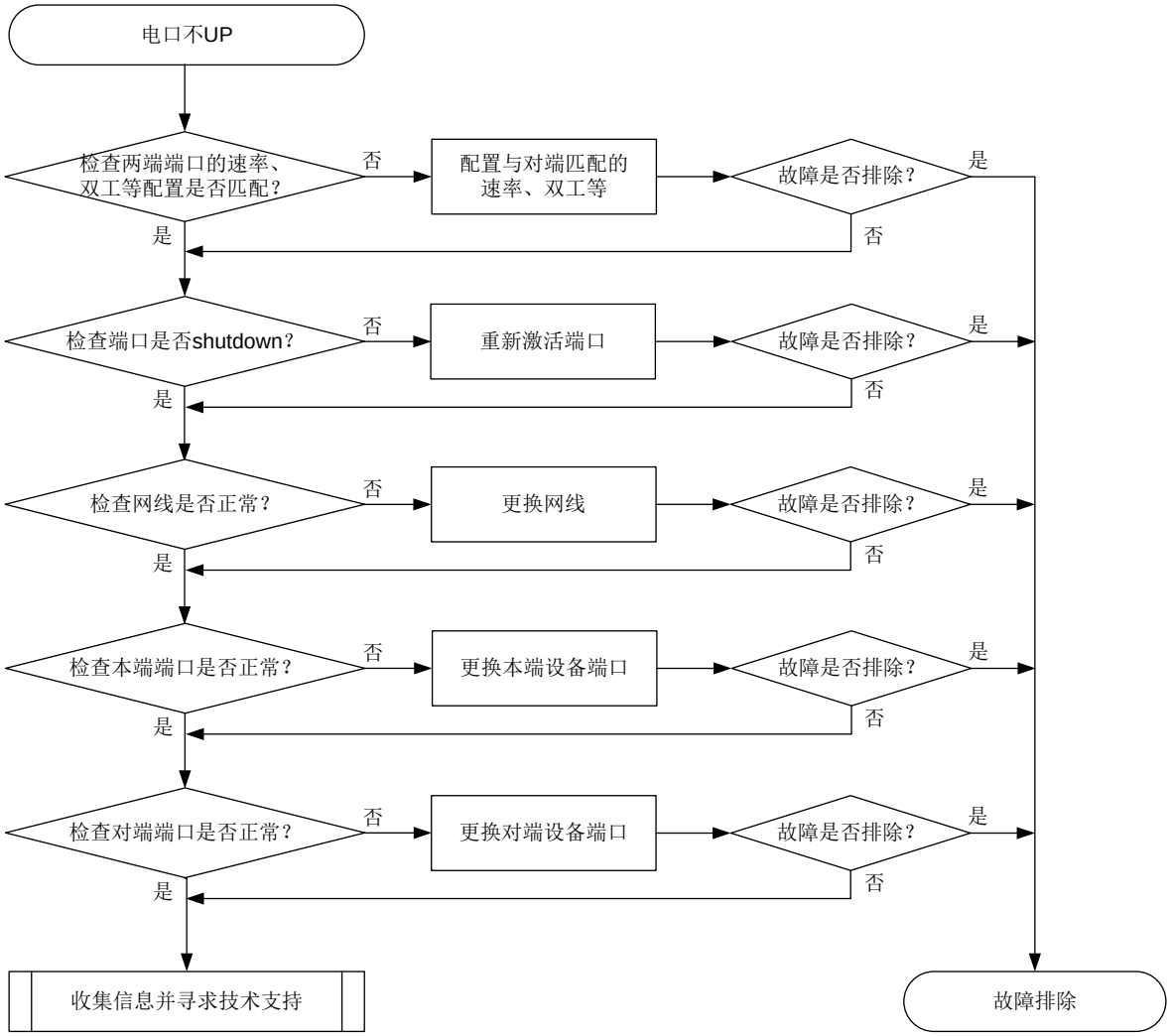
本类故障的常见原因主要包括：

- 端口配置问题。
- 网线有问题。
- 本端或者对端端口有问题。

3. 故障分析

本类故障的诊断流程如图 12 所示：

图12 故障诊断流程图



4. 处理步骤

(1) 查看网线两端对接设备网口配置（端口速率，双工，协商模式等）是否一致。执行 **display interface brief** 命令，查看两端端口的速率、双工配置是否匹配。若不匹配，请通过 **speed** 命令和 **duplex** 命令配置端口的速率和双工模式。

```
<Sysname> 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
GE1/0/1              DOWN DOWN     --
Loop0                UP   UP(s)    2.2.2.9
NULL0                UP   UP(s)    --
Vlan1                UP   UP       --
Vlan999              UP   UP       192.168.1.42
```

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link   Speed   Duplex   Type   PVID  Description
GE1/0/2              DOWN   auto    A        A      1     aaaaaaa
GE1/0/3              UP     1G(a)   F(a)     A      1     aaaaaaa
```

(2) 通过 **display interface** 命令查看端口状态 Current state 是否为 Administratively DOWN 状态，如果是，请使用 **undo shutdown** 命令激活相应的以太网端口。

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
...
```

(3) 更换一根确认为好的网线，检查故障是否排除。

(4) 分别更换本端设备端口以及对端设备端口，检查故障是否排除。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

2.4.5 端口频繁 UP/DOWN

1. 故障描述

板卡插入线缆或光模块后，端口频繁 UP/DOWN。

2. 常见原因

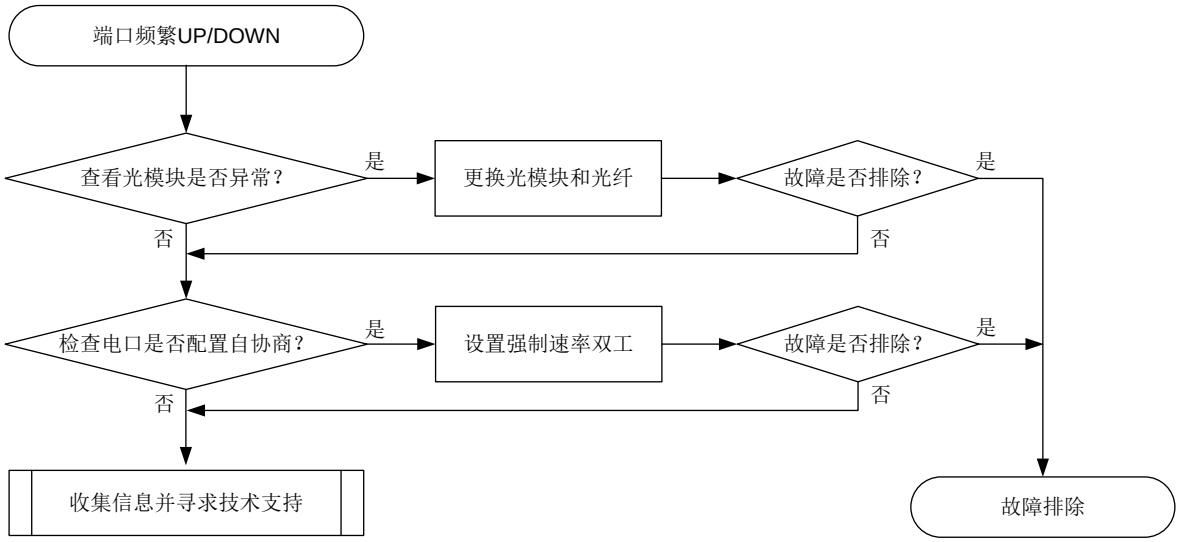
本类故障的常见原因主要包括：

- 光模块或线缆故障
- 电口自协商不稳定

3. 故障分析

本类故障的诊断流程如图 13 所示：

图13 故障诊断流程图



4. 处理步骤

(1) 对于光口，需要确认光模块是否异常。通过查看光模块 alarm 信息来排查两者光模块以及中间光纤问题。告警信息中如果存在接收有问题那一般是对端端口、光纤或中转传输设备导致；如果是发送有问题或者电流、电压异常那就需要排查本端端口。

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver current alarm information:
  RX loss of signal
  RX power low
```

(2) 检查光模块的接收、发送光功率是否正常（即在该光模块的光功率上下门限值之内）。如果发送光功率处于临界值，请更换光纤、光模块做交叉验证；如接收光功率处于临界值，请排查对端光模块及中间光纤链路。

```
<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36        3.31        6.13      -35.64          -5.19
  Alarm thresholds:
            Temp(°C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High    50         3.55        1.44      -10.00         5.00
    Low     30         3.01        1.01      -30.00         0.00
```

(3) 对于电口，一般在自协商情况下容易出现协商不稳定，这种情况请尝试设置强制速率双工。

(4) 如果故障依存在，请排查链路、对端设备、中间设备。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

2.5 光模块故障

2.5.1 光口不 UP 故障

1. 故障描述

光口不 UP。

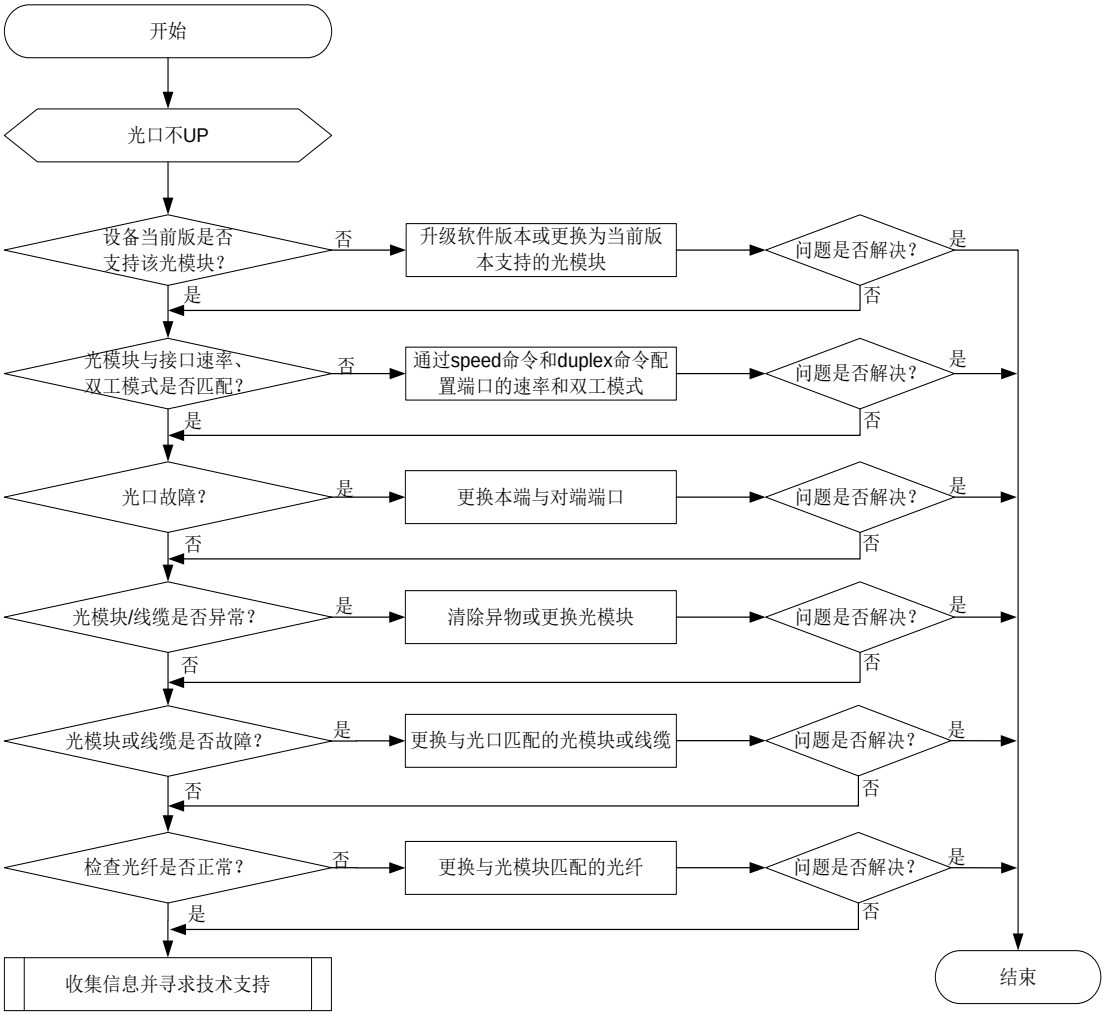
2. 常见原因

- 设备当前版本不支持该光模块。
- 光口有异物或光模块金手指被污染、损坏。
- 光模块与接口速率不匹配。
- 光口故障。
- 光模块或线缆故障。
- 光模块与光纤类型不匹配。

3. 故障分析

本类故障的诊断流程如 2.4.1 3. 图 9所示。

图14 故障诊断流程图



4. 处理步骤

(1) 检查设备当前版本是否支持该光模块。

可通过产品安装手册或软件版本说明书查看当前软件版本是否支持该光模块。如果有新版本支持该光模块，也可以升级软件版本。

(2) 检查光模块与接口速率、双工模式是否匹配。

执行 **display interface** 命令，查看端口与光模块的速率、双工配置是否匹配。若不匹配，请通过 **speed** 命令和 **duplex** 命令配置端口的速率和双工模式。

(3) 检查光接口是否故障。

在本设备上的相同速率的光口上用匹配的线缆（适用于短距离连接）直接互连，查看该端口是否能 UP。如果能 UP，则说明对端端口异常；如果不能 UP，则说明本端端口异常。可通过更换本端与对端端口来检查故障是否解决。

(4) 检查光模块/线缆是否异常。

可通过如下步骤检查光模块/线缆是否异常：

a. 可通过 **display transceiver alarm interface** 命令，查看当前端口上的光模块的故障告警信息，若显示为“None”，则表示没有故障；若显示有告警信息，可通过查看光模块/线缆告警信息来确认是光模块问题还是光纤或者对端问题。比如出现 RX signal loss 和 TX fault 错误，可以查看光口、光模块是否存在异物，或者光模块金手指严重氧化。

b. 可通过 **display transceiver interface** 命令，检查两端的光模块类型、波长、传输距离等参数是否一致。

c. 可通过 **display transceiver diagnosis interface** 命令，检查光模块的数字诊断参数的当前测量值是否在正常范围内。参数异常常见问题及解决办法如下：

- 当光纤与光模块接触不良时，可通过将光线与光模块插牢解决。
- 当光纤质量不好或损坏，可通过更换光纤解决。
- 当传输路径增加了中间光衰设备，可根据实际使用，调整光衰设备解决。
- 当光模块适配传输距离与实际使用距离相差较大，更换为与实际传输距离适配的光模块解决。

(5) 检查光模块类型与光纤是匹配。

可通过《H3C 光模块手册》，查看光模块类型与光纤类型是否匹配。若不匹配，可通过更换光纤解决。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

- OPTMOD/3/CFG_ERR
- OPTMOD/5/CHKSUM_ERR
- OPTMOD/5/IO_ERR
- OPTMOD/4/FIBER_SFPMODULE_INVALID
- OPTMOD/4/FIBER_SFPMODULE_NOWINVALID
- OPTMOD/5/MOD_ALM_ON
- OPTMOD/5/RX_ALM_ON
- OPTMOD/5/RX_POW_HIGH
- OPTMOD/5/RX_POW_LOW

2.5.2 光模块上报非 H3C 合法光模块故障处理

1. 故障描述

通过 **display logbuffer** 命令查看系统日志时，发现存在上报非 H3C 合法光模块的相关信息。相关日志信息显示如下：

```
This transceiver is NOT sold by H3C. H3C  therefore shall NOT guarantee the normal function of the device or  assume the maintenance responsibility thereof!
```

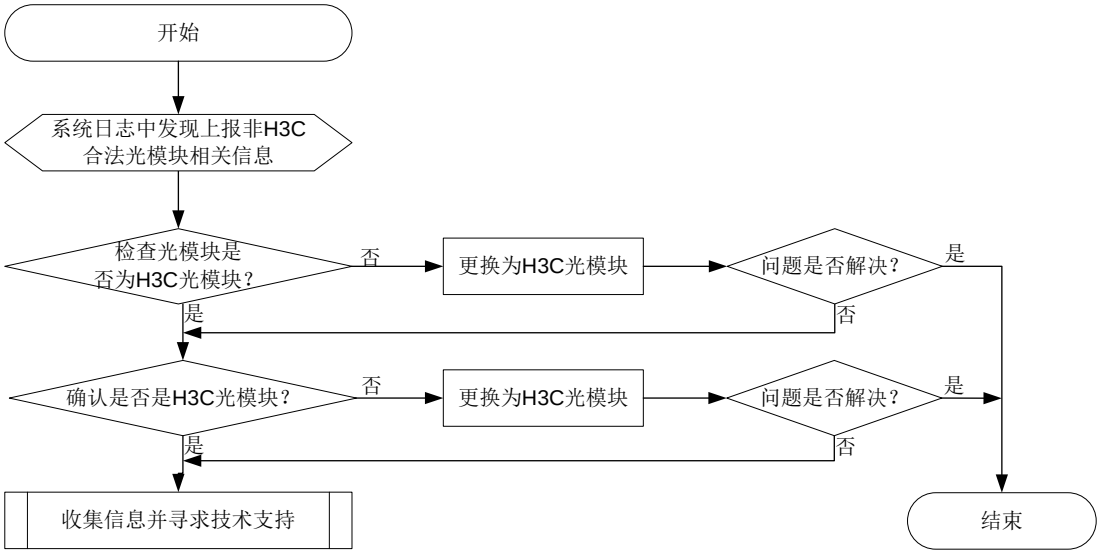
2. 常见原因

光模块为第三方光模块或伪造的 H3C 光模块。

3. 故障分析

本类故障的诊断流程如图 15 所示。

图15 故障诊断流程图



4. 处理步骤

(1) 检查光模块是否为 H3C 光模块。

a. 根据光模块上的标签判断是否为 H3C 认证光模块。

b. 通过命令 **display transceiver interface**，查看 Vendor Name 是否是 H3C。如果显示的是 H3C，则可能是没有电子标签的 H3C 光模块，也可能不是 H3C 光模块，需要进一步确认。如果显示的是其它信息，则一定不是 H3C 光模块，可通过更换为 H3C 光模块来检查故障是否排除。

(2) 与 H3C 的技术支持工程师确认是否是 H3C 光模块。

通过 Probe 视图下的命令 **display hardware internal transceiver register interface** 和 **display transceiver information interface** 收集光模块信息。然后向H3C技术支持工程师反馈光模块上的条码，确认光模块的渠道来源，明确是否是H3C光模块。如果确认不是 H3C 光模块，可通过更换为 H3C 光模块来检查故障是否排除。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

- OPTMOD/4/PHONY_MODULE

2.5.3 光模块不支持数字诊断

1. 故障描述

通过 **display transceiver diagnosis interface** 命令查看光模块诊断信息时，系统提示光模块不支持数字诊断。显示如下：

```
<Sysname> display transceiver diagnosis interface GigabitEthernet 1/0/1
The transceiver does not support this function.
```

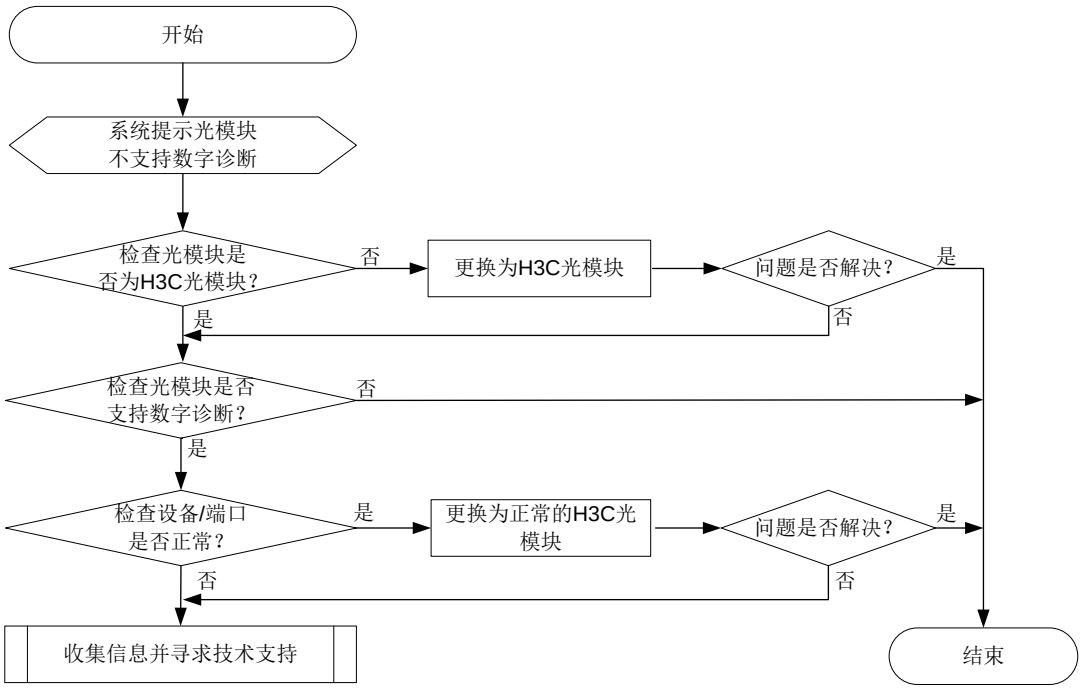
2. 常见原因

- 光模块为非 H3C 光模块。
- 光模块不支持数字诊断。
- 光模块故障。
- 设备/光口故障。

3. 故障分析

本类故障的诊断流程如图 16 所示。

图16 故障诊断流程图



4. 处理步骤

(1) 判断是否为 H3C 光模块，具体步骤见 2.5.2 光模块上报非 H3C 合法光模块故障处理。

(2) 通过 **display transceiver interface** 命令，查看 Digital Diagnostic Monitoring 字段是否是 YES，如果是 YES，表明支持数字诊断，反之亦然。

(3) 使用相同型号光模块插在本设备其他正常端口或者其他正常运行且支持该光模块的设备上，检查是否仍然提示不支持数字诊断。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

2.5.4 光模块序列号丢失

1. 故障描述

使用 **display transceiver manuinfo interface** 命令查看光模块序列号丢失。

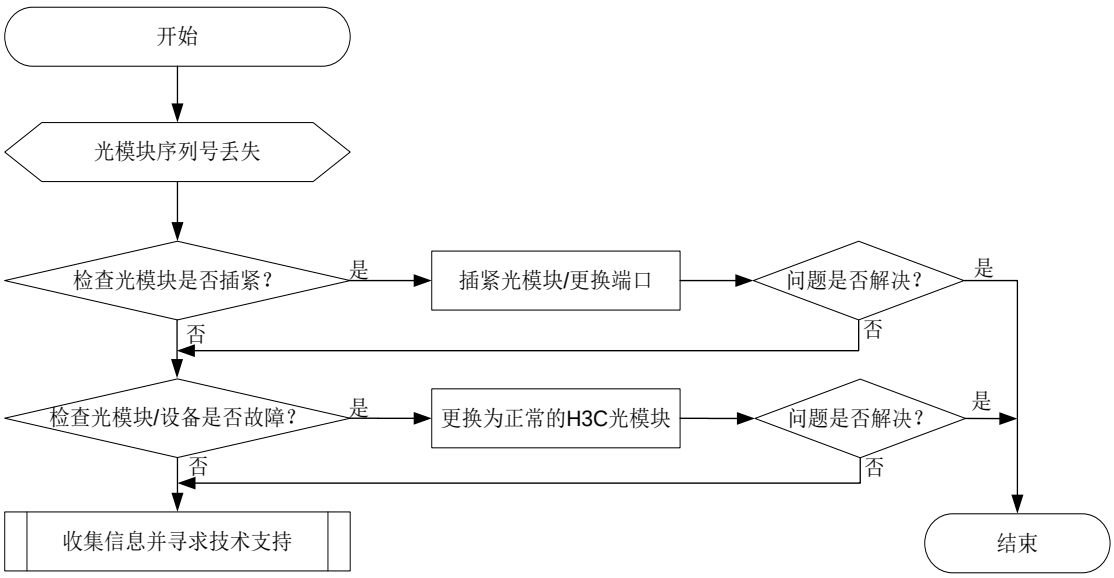
2. 常见原因

- 光模块未插紧。
- 光模块/设备故障。

3. 故障分析

本类故障的诊断流程如图 17 所示。

图17 故障诊断流程图



4. 处理步骤

(1) 检查光模块是否完全插入光口。

可通过插紧光模块，或更换光口解决。

(2) 检查光模块是否故障。

可通过使用相同型号光模块插在本设备端口或者其他正常运行且支持该光模块的设备上来判断。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

2.6 PoE供电故障

2.6.1 PoE 供电异常

1. 故障描述

PoE 供电功率不足或无法供电。

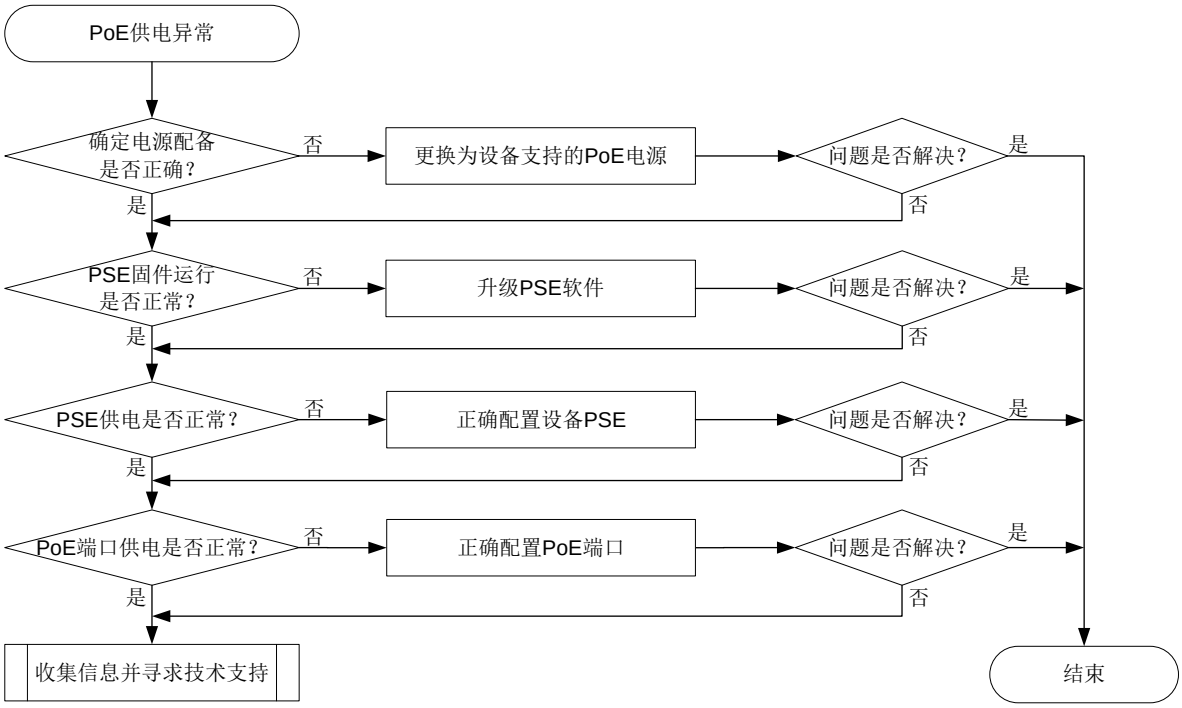
2. 常见原因

- 供电电源与设备不匹配或供电电源供电能力不足。
- PSE 固件故障。
- 受电设备为非标准 PD，PoE 接口没有开启非标准 PD 检测功能。

3. 故障分析

本类故障的诊断流程如图 18 所示。

图18 故障诊断流程图



4. 处理步骤

(1) 确定电源配备是否正确。

检查设备配备的电源模块，对于 PoE 设备，必须按照电源配置方案配置电源。关于电源模块的适配情况，请参见对应产品的安装指导或硬件描述。

(2) 查看 PSE 固件运行是否正常。

a. 执行 **display poe device** 命令查看 PSE 的工作状态。如果工作状态显示为 Faulty，则说明 PSE 故障。如下所示：

```
<Sysname> display poe device
Slot  1:
 PSE ID  Slot No. SSlot No. PortNum  MaxPower(W)  State  Model
 1       0        0         48       0            Faulty LSP1POEA
```

以上显示信息说明该 PSE 存在故障。

b. 联系 H3C 技术支持人员或设备供应商获取对应版本的 PSE 固件，然后执行 **poe update** 命令升级 PSE 固件。升级方法如下所示：

```
<Sysname> system-view
[Sysname] poe update full POE-168.bin pse 4
This command will refresh the PSE firmware. Continue? [Y/N]:y
……
```

以上显示信息说明 PSE 软件升级成功。

c. 再次执行 **display poe device** 命令查看 PSE 的工作状态。如果工作状态显示为 on 或 off，则说明 PSE 故障已修复。如下所示：

```
[Sysname] display poe device
Slot  1:
```

```
PSE ID  Slot No. SSlot No. PortNum  MaxPower(W)  State  Model
1       0        0         48       0            on     LSP1POEA
```

(3) 在任意视图中执行 **display poe pse** 命令查看 PSE 的信息。确认当前整机供电功率、平均功率、峰值功率是否正常、PSE 检测非标准 PD 功能是否打开等。如下所示：

```
<Sysname> display poe pse
 PSE ID                                  : 1
 Slot NO.                                : 0
 PSE Model                               : LSBMPOEGV48TP
 PSE Status                              : Enabled
 PSE Preempted                           : No
 Power Priority                          : Low
 Current Power                           : 130      W
 Average Power                           : 20       W
 Peak Power                              : 240      W
 Max Power                               : 200      W
 Remaining Guaranteed Power             : 120      W
 PSE CPLD Version                         : 100
 PSE Software Version                    : 200
 PSE Hardware Version                    : 100
 Legacy PD Detection                      : Disabled
 Power Utilization Threshold            : 80
 PSE Power Policy                         : Disabled
 PD Power Policy                          : Disabled
 PD Disconnect-Detection Mode           : DC
```

- 如果 PSE 当前供电功率、PSE 平均功率、PSE 峰值功率都达到或接近 PSE 最大供电功率，说明 PoE 电源模块供电不足，此时请选配更大供电功率的 PoE 电源模块。
- 如果 PSE Legacy PD Detection 字段显示为 Disable，请执行 poe legacy enable 命令，开启非标准 PD 检测功能。

(4) 在任意视图中执行 **display poe interface** 命令查看 PoE 端口的相关信息。确认当前端口供电功率、平均功率、峰值功率是否正常，端口的电流、电压是否正常。如下所示：

```
<Sysname> display poe interface gigabitethernet 1/0/1

 PoE Status                      : Enabled
 Power Priority                  : Critical
 Oper                            : On
 IEEE Class                      : 1
 Detection Status                : Delivering power
 Power Mode                      : Signal
 Current Power                   : 11592    mW
 Average Power                   : 11610    mW
 Peak Power                      : 11684    mW
 Max Power                       : 15400    mW
 Electric Current                : 244      mA
 Voltage                         : 51.7     V
 PD Description                  : IP Phone For Room 101
```

如果当前端口供电功率、平均功率、峰值功率都达到或接近端口最大供电功率，说明 PoE 端口供电不足，此时请执行 **poe max-power** 命令重新配置 PoE 端口的最大供电功率。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

2.7 E1&T1接口故障处理

2.7.1 E1&T1 常见排查方法

E1/T1 常见排查方法有：

- 硬件排查。
- 线缆排查。
- 配置排查。
- 时钟排查。
- 接地排查。
- 打环排查。

1. 硬件排查方法

(1) 确认外接电源连接：

对问题主机进行独立供电测试以排除电源问题。

(2) 本地自环测试：

在 E1/T1 接口下配置 **loopback local** 命令或在 E1-F/T1-F 接口视图下配置 **fe1 loopback local/ft1 loopback local** 命令观察接口物理是否 up，并观察逻辑串口上的收发是否正确环回，如果正常可以初步排除板卡硬件问题。

a. 如果接口本地自环失败，并且在更换槽位后本地自环成功，可以定位为硬件问题，将问题主机走分析件流程。

b. 更换单板测试，如果接口本地自环失败，并且在更换单板后本地自环成功，可以定位为硬件问题，将问题单板走分析件流程。

c. 更换主机测试，如果接口本地自环失败，并且在更换主机后本地自环成功，可以定位为硬件问题，将问题主机走分析件流程。

2. 线缆排查方法

(1) 线缆质量排查

- 确保线缆为我司标准线缆。
- 更换电缆。

- 将电缆收发短接，查看接口是否能成功自环。若自环成功，可排除线缆问题。如何查看自环请参见 2.7.1 6. 打环排查方法。

(2) 排查线缆阻抗与接口阻抗是否匹配

- 通过 **display controller** 或 **display fe1** 获取接口阻抗（例文中蓝色字体）：

```
<Sysname> display controller E1 1/0/0
E1 1/0/0 current state :DOWN
Description : E1 1/0/0 Interface
Basic Configuration:
    Work mode is E1 framed, Cable type is 120 Ohm balanced.
```

- 通过更换线缆或调整接口卡拨码开关（HMIM-8E1T1 板卡使用硬件跳线和 **cable-type** 命令确认板卡阻抗类型）来保证线缆阻抗和接口阻抗的一致性。

接口类型：E1 接口

相应命令：**cable-type** { **75** | **120** }

参数说明：75：匹配 75 欧的传输线路；120：匹配 120 欧的传输线路。

(3) 排查线缆长度与配置是否匹配

E1/T1 接口对其使用的电缆长度有一定的限制，通常最大长度不能超过 500 米，当线缆越长，信号衰减越大，此时需对信号进行补偿或外接 CSU 设备，路由器提供了 **cable** 命令用来设置接口匹配的传输线路的衰减或长度，本命令作用是配置发送时的信号波形，以适应不同传输需要。实际使用中，可根据接收端收到的信号质量的好坏，来决定是否使用此命令。如果信号质量较好，可以使用缺省设置。

接口类型：E1 接口

相应命令：**cable** { **long** | **short** }

参数说明：**long**：匹配 655 英尺以上的传输线路；**short**：匹配 655 英尺以下的传输线路。

接口类型：T1/T1-F 接口

相应命令：**cable** { **long** *decibel* | **short** *length* }

参数说明：

long *decibel*：匹配 655 英尺以上的传输线路。参数 *decibel* 的值可以为 **0db**、**-7.5db**、**-15db**、**-22.5db**，用户可根据接收端信号质量选择不同的衰减参数。当线路质量越差时，信号衰减越大，需要用户对这种衰减进行相应补偿，此时，不需要外接 CSU。

short *length*：匹配 655 英尺以下的传输线路。参数 *length* 的值可以为 **133ft**、**266ft**、**399ft**、**533ft**、**655ft**，用户可根据传输线路的长度，选择相应的长度参数。

3. 配置排查方法

(1) 通信两端配置要保持一致：

包括工作模式（成帧或非成帧）、帧格式、CRC 校验方式、编码格式、线路空闲码、帧间填充符。

提示

CISCO E1 接口默认帧格式为 CRC4，我司 E1 接口默认帧格式为 NO-CRC4，两者互联时请使之保持一致。

---

(2) 用配置解决 AIS 告警误检问题：

如果线路上正常传输的数据为全 1 码流，空闲码为 FF，当没有业务数据传输时，线路上传输的数据为全 1 的空闲码，即表现为 AIS 告警。

两种解决方案：

- 在路由器上配置 **undo detect-ais** 命令，即不检测 AIS 命令。
- 把帧间填充改为 7E。

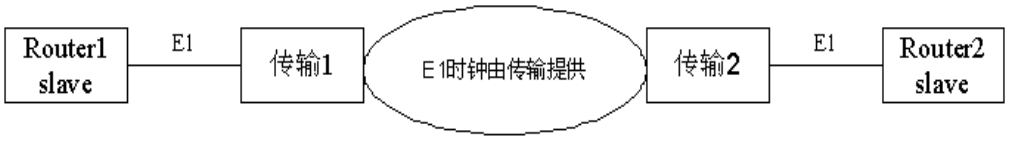
4. 时钟排查方法

(1) 标准时钟方案

根据传输网络是否提供时钟，E1 有两类时钟方案：

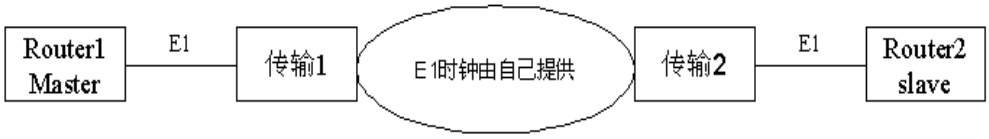
- 当传输网络提供时钟时，即传输为主时钟，E1 对接双方都为从时钟。

图19 传输提供时钟时 E1 时钟配置方案



- 当传输网络不提供时钟时，即传输只进行透传，此时 E1 对接双方应一端配置主时钟，另一端配置从时钟。

图20 传输不提供时钟时 E1 时钟配置方案



(2) 频偏测量

如果时钟配置有误，会导致线路上时钟产生频偏。E1 接口正常的频偏范围为正负 50ppm，如果频偏超过这个范围，则不能保证数据收发正常。频偏有积累效应，即频偏会随着时间推移持续变大，表现为 E1 接口由正常到出现错包，直至到不可用状态。可通过 **shutdown/undo shutdown** 命令使频偏回到初时值，恢复接口使用。

通常，可以使用 ETEN 表来测量线路的频偏，方法为将 ETEN 串接在 E1 的接收或发送线路上，分别测试线路的收发频偏。

5. 接地排查方法

(1) 常见的不良接地和共地

- 设备安装在 19 英寸机柜中，但并未将设备的地线接到机柜的接地线上。
- 设备与对接设备在同一机房，设备只接地，但并未共地。

(2) 不良共地的影响

共地不良会导致对接双方基准电压不同，数据的收发和各种信号的检测不在一个电压平台上。于是，会出现本端发送的数据与对端接收的数据不一致，收发出现错包，严重时会导致协议

up/down，或者本端正常的发送信号，对方无法检测或错误检测，导致物理上出现告警，E1 物理接口 up/down。

(3) 接地要求

- 设备必须接地。
- 如果设备与对接设备在同一机房，设备不但要接地，还要与对接设备共地。
- 接地导线必须采用铜导线以降低高频阻抗，接地线尽量粗和短，接地线不得使用铝材。
- 接地线两端的连接点应确保电气接触良好，并做防腐、防锈处理。
- 不得利用其他设备作为接地线电气连通的组成部分。
- 接地引线不能与信号线平行走线或相互缠绕。
- 保护地线上严禁接头，严禁加装开关或熔断器。
- 保护地线应选用黄绿双色相间的塑料绝缘铜芯导线。
- 保护地线的长度不应超过 30 米，且尽量短，当超过 30 米时，应要求客户就近重新设置地排。
- 设备如果用 UPS 供电，那么 UPS 也必须接地。

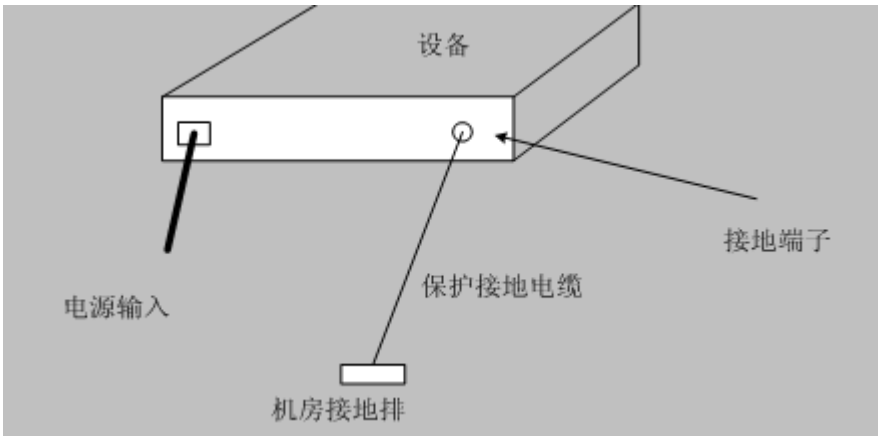
可靠接地是设备具有良好的防雷、防电击和抗干扰性能的基本要求，是设备长期可靠、稳定运行的前提。

(4) 不同环境中设备接地方法

- 安装环境中提供接地排

当设备所处安装环境中有接地排时，在确认接地排的接地连接可靠的情况下，将设备黄绿双色的保护接地电缆一端接至接地排的接线柱上，拧紧固定螺母（如图 3-11 所示）。保护接地电缆截面积必须不小于 4mm^2，工程施工时该电缆尽量短，不能盘绕。

图21 机房有接地排时接地安装简图



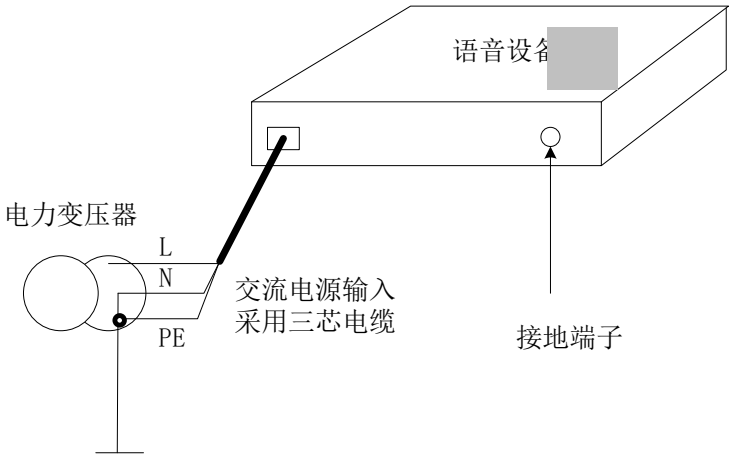
对于安装在 19 英寸机柜上的设备，可将设备黄绿双色的保护接地电缆接到 19 英寸机柜的接地端子上，并确认 19 英寸机柜的接地端子与机房接地排可靠连接。

- 安装环境中无接地排，并且条件不允许埋设接地体

当设备所处安装环境中没有接地排，并且条件不允许埋设接地体时。

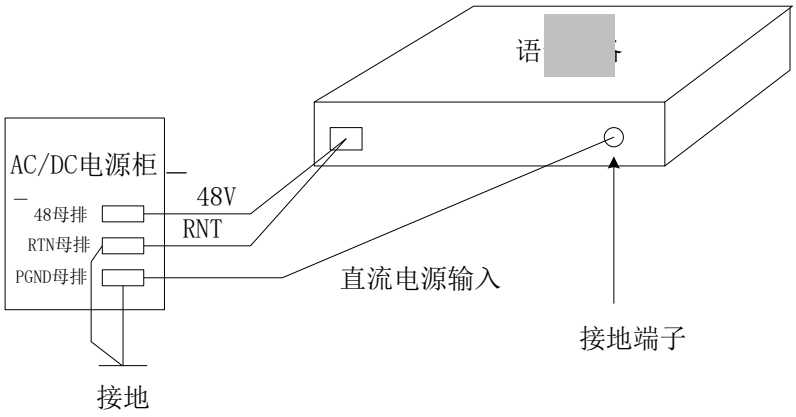
- 若设备采用 220V 交流电供电，可以通过交流电源的 PE 线进行接地（如图 3-12 所示）。确认交流电源的 PE 线在配电室或交流供电变压器侧是否良好接地，并保证设备的 PE 端子可靠的和交流电源的 PE 线连接，设备的电源电缆应采用带保护地线的三芯电缆。若交流电源的 PE 线在配电室或交流供电变压器侧没有接地，应及时向客户提出整改的要求。

图22 利用交流 PE 线接地时接地安装简图



- 若设备采用-48V（或+24V）直流电供电，可以通过直流电源的回流线 RTN 或 PGND 进行接地（如图 3-13 所示）。确认 RTN 或 PGND 在直流电源柜的直流输出口处是可靠接地的，若 RTN 或 PGND 在直流电源柜的直流输出口处没有接地，应及时向客户提出整改的要求。

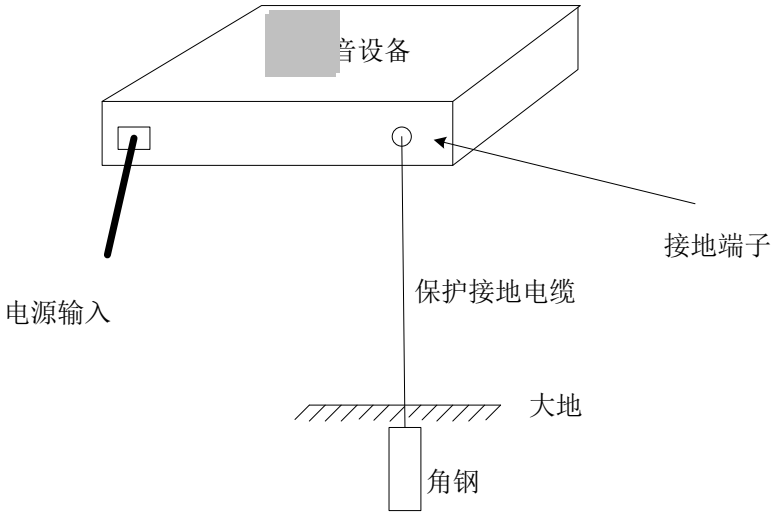
图23 利用电源柜 PGND 接地时接地安装简图



安装环境中无接地排，附近可以埋设接地体

- 当设备所处安装环境中没有接地排，附近有泥地并且允许埋设接地体时，可采用长度不小于 0.5m 的角钢或钢管，直接打入地下。 角钢截面应不小于 L×W×H = 50×50 ×5mm，钢管壁厚应不小于 3.5mm，材料采用镀锌钢材。设备黄绿双色的保护接地电缆应和角钢采用电焊连接，焊接点表面应涂敷防锈漆进行防锈处理。 保护接地电缆截面积必须不小于 4mm2，工程施工时该电缆尽量短，不能盘绕（如图 3-14 所示）。

图24 机房附近允许埋设接地体时接地安装简图



注意

（3）的方法较简易，接地电阻可能会很高，若(1)和(2)的接地条件均不具备，才可采用此接地方式。

(5) 接地电阻值

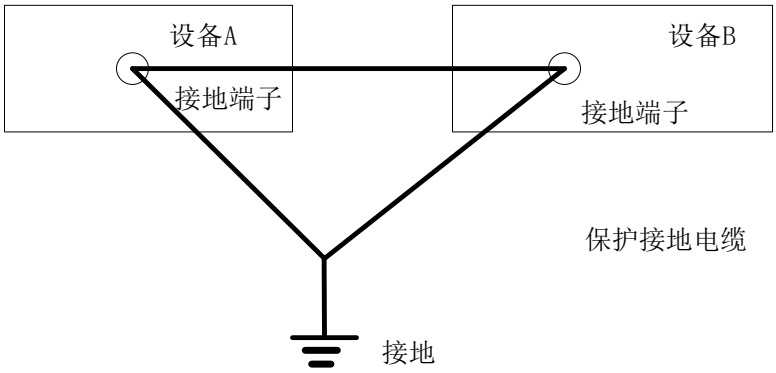
设备接地连接的机房接地排，其接地电阻应按照机房环境的要求来确定。对于电信中心机房，接地电阻按照 YDJ26-89 标准要求执行（标准要求小于 1Ω）；对于非电信中心机房，接地电阻应小于 5Ω；对于打入地下的角钢，其接地电阻可适当放宽，应小于 10Ω。对于土壤电阻率高的地方，宜在接地体泥土周围撒一些盐水或降阻剂等措施来降低土壤的电阻率。

(6) 设备共地方法

对接设备之间一定要共地，同时各对接设备也要可靠接地。

- 如果对接设备都安装在 19 英寸机柜中，那么分别把对接设备的地线直接接到机柜的接地线上共地。
- 如果对接设备之间放置在同一个机房内，且距离不太远，那么可以通过把对接设备的接地线直接连接在一起，然后再接地的方法来共地，如下图所示。

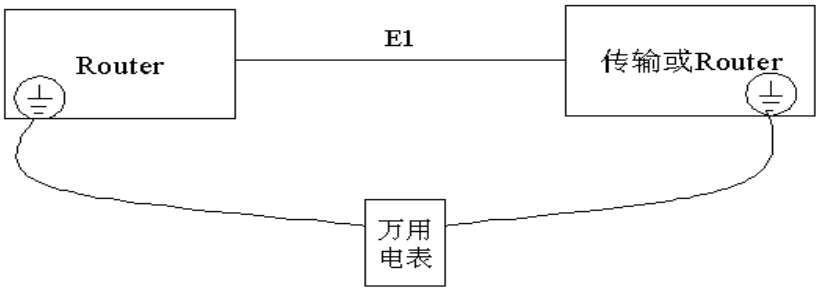
图25 设备共地示意图



- 如果对接设备没有安装在同一个机房，无法通过接地线共地，那么采用对接设备分别可靠接地的方法来共地。

(7) 共地是否可靠的测量方法

图26 共地是否可靠的测量方法



按上图用接地线将对接设备的接地点引出，用万用电表测量这两点的电压和电阻：

良好的接地：被测两点的电阻应迅速归零，而电压值小于 1V。

不良的接地：被测两点之间电阻值非零，或虽为零但并未迅速归零，或两点电压值大于 1V。

6. 打环排查方法

(1) 常用的打环点

图27 共地是否可靠的测量方法

- 1 打环点：

  打环方法：在路由器上 E1 接口上配置 **loopbace local**，在 FE1 接口下配置 FE1 **loopbace local**。

测试目的：排查路由器接口本身收发是否正常。

- 2、3 打环点：

  打环方法：将 Router1 与传输 1 之间的 E1 收发线缆短接或在传输上向左侧打环。

  测试目的：排查 Router1 和传输 1 之间线路是否正常。

- 4 打环点：

  打环方法：在传输 2 上向左侧打环。

  测试目的：排查传输网络是否正常。

- 5 打环点：

  打环方法：将 Router1 与传输 1 之间的 E1 收发线缆短接。

  测试目的：排查 Router1 到 Router2 直接整个物理链接是否正常。

- 6 打环点：

  打环方法：在 Router2 上 E1 接口上配置 **loopbace remote**/**loopbace payload**，在 FE1 接口下配置 **fe1 loopbace remote**/**fe1 loopbace payload**。

  测试目的：排查整个链路，包括 Router2 是否正常。

(2) 打环后如何进行线路排查：

- 通过路由器自环检测功能进行排查

  将接口链路层协议配置为 PPP，查看接口收发以 12 个包的步长匀速增长，在接口信息中显示 loopback is detected，而且接口上没有错包增加，则表明链路正常，否则为异常。

```
<Sysname> display interface serial 1/0:0
Serial1/0:0
Current state: UP
Line protocol state: DOWN
Description: Serial1/0:0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds, retry times: 5
Derived from E1 1/0, Timeslot(s) Used: 1, Baudrate is 64000 bps
Internet protocol processing: disabled
Link layer protocol: PPP, Loopback: detected
LCP: closed
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Last 300 seconds output rate: 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Input:
  12 packets, 156 bytes
  0 broadcasts, 0 multicasts
  0 errors, 0 runts, 0 giants
  0 CRC, 0 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  12 packets, 156 bytes
```

```
0 errors, 0 underruns, 0 collisions
0 deferred
```

- 通过误码仪进行排查

  用线路误码仪取代路由器的位置，将接在路由器上的收发线缆接在误码仪的收发上，此时误码仪即能显示线路上是否有误码存在。

2.7.2 E1&T1 常见问题定位

常见的 E1/T1 模块问题可以分为以下两类：

- 物理接口异常，表现为controller接口信息存在LOS、LFA、AIS或RAI告警，物理一直down或反复 up/down。
- 物理接口 UP，并且没有告警，但数据收发异常，表现为对接双方接口上有错包或链路层协议up/down。

1. 物理接口异常问题

- 故障描述

物理接口异常，表现为 controller 接口信息存在 LOS、LFA、AIS 或 RAI 告警，物理一直 down 或反复 up/down。

- 故障处理步骤

按如下顺序进行问题排查

(1) 用硬件排查方法排查硬件问题。

(2) 用线缆排查方法排查线缆问题。

(3) 用配置排查方法排查配置问题。

(4) 用时钟排查方法排查时钟问题。

(5) 用接地排查方法排查接地问题。

(6) 用打环排查方法排查线路问题。

2. 数据收发异常问题

- 故障描述

物理接口UP，并且没有告警，但数据收发异常，表现为对接双方接口上有错包或链路层协议up/down。

- 故障处理步骤

按如下顺序进行问题排查

(1) 用硬件排查方法排查硬件问题。

(2) 用线缆排查方法排查线缆问题。

(3) 用配置排查方法排查配置问题。

(4) 用时钟排查方法排查时钟问题。

(5) 用接地排查方法排查接地问题。

(6) 用打环排查方法排查线路问题。

3. 信息收集建议

如果上述步骤无法定位或排除故障，请收集如下信息，并联系 H3C 技术支持人员：

- **display diagnostic-information**
- **display device verbose**

- **display controller**、**display fe1** 或 **display ft1**
- **display interface serial**(如收发有错包增长，请有间隔的多次收集该信息)

2.8 以太接口故障处理

2.8.1 无法 ping 通直连设备问题

1. 故障描述

无法 ping 通与以太网接口直连的设备。

2. 故障处理步骤

(1) 通过 **display interface** 命令收集指定接口信息，查看：

- 接口状态是否 UP。
- 接口两端速率双工是否匹配。
- 接口收发包统计是否正常，有无错包和丢包统计，如果有错包统计，可以先排除线缆问题或接口故障。
- 如果接口是光口查看两端光模块是否匹配。

(2) 通过 **display arp all** 命令查看是否学到直连接口的 ARP，如果没有，通过 **debugging arp packet** 命令打开两台设备上的 ARP 调试开关，查看 ARP 收发是否存在异常情况。

(3) 通过 **debugging ip packet** 命令打开两个设备上的 IP 调试开关，通过 **debugging ip icmp** 命令打开 ICMP 调试开关，查看 ICMP 收发是否存在异常情况。

(4) 如果上述步骤无法具体定位故障，请联系 H3C 技术支持人员。

2.8.2 转发不通问题

1. 故障描述

以太网接口所在路由器作为中间设备转发流量时，流量转发不通。

2. 故障处理步骤

(1) 在没有流量转发的情况下，确认以太网接口与直连设备是否可以 ping 通，如果不通，请参见 2.8.1 无法 ping 通直连设备问题处理。

(2) 通过 **debugging ip packet** 命令打开设备上的 IP 调试开关，查看 IP 报文收发是否存在异常情况。

(3) 如果上述步骤无法具体定位故障，请联系开发人员。

2.8.3 转发丢包问题

1. 故障描述

以太网接口转发流量有丢包问题。

2. 故障处理步骤

(1) 通过 **display counters rate inbound interface** 命令查看入接口速率统计，通过 **display counters rate outbound interface** 命令查看出接口速率统计，初步确认丢包的设备。

(2) 通过 **display interface** 命令查看流量出接口统计，查看 qos 队列入方向是否有流量，是否有丢包。

(3) 如果上述步骤无法具体定位故障，请联系 H3C 技术支持人员。

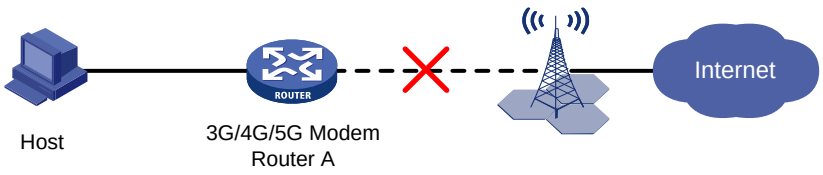
3. 故障诊断命令

命令	说明
display interface	查看接口信息
display arp all	查看所有的ARP表项信息
display counters rate inbound interface	查看入接口速率统计
display counters rate outbound interface	查看出接口速率统计
debugging arp packet	打开ARP的报文调试信息开关
debugging ip packet	打开IP报文调试信息开关
debugging ip icmp	打开ICMP调试信息开关

3 3G/4G/5G 链路故障处理

3.1 故障描述

MSR 路由器使用 3G/4G/5G 接口模块接入 Internet，局域网用户无法上网，3G/4G/5G 接口模块 WWAN 指示灯异常。



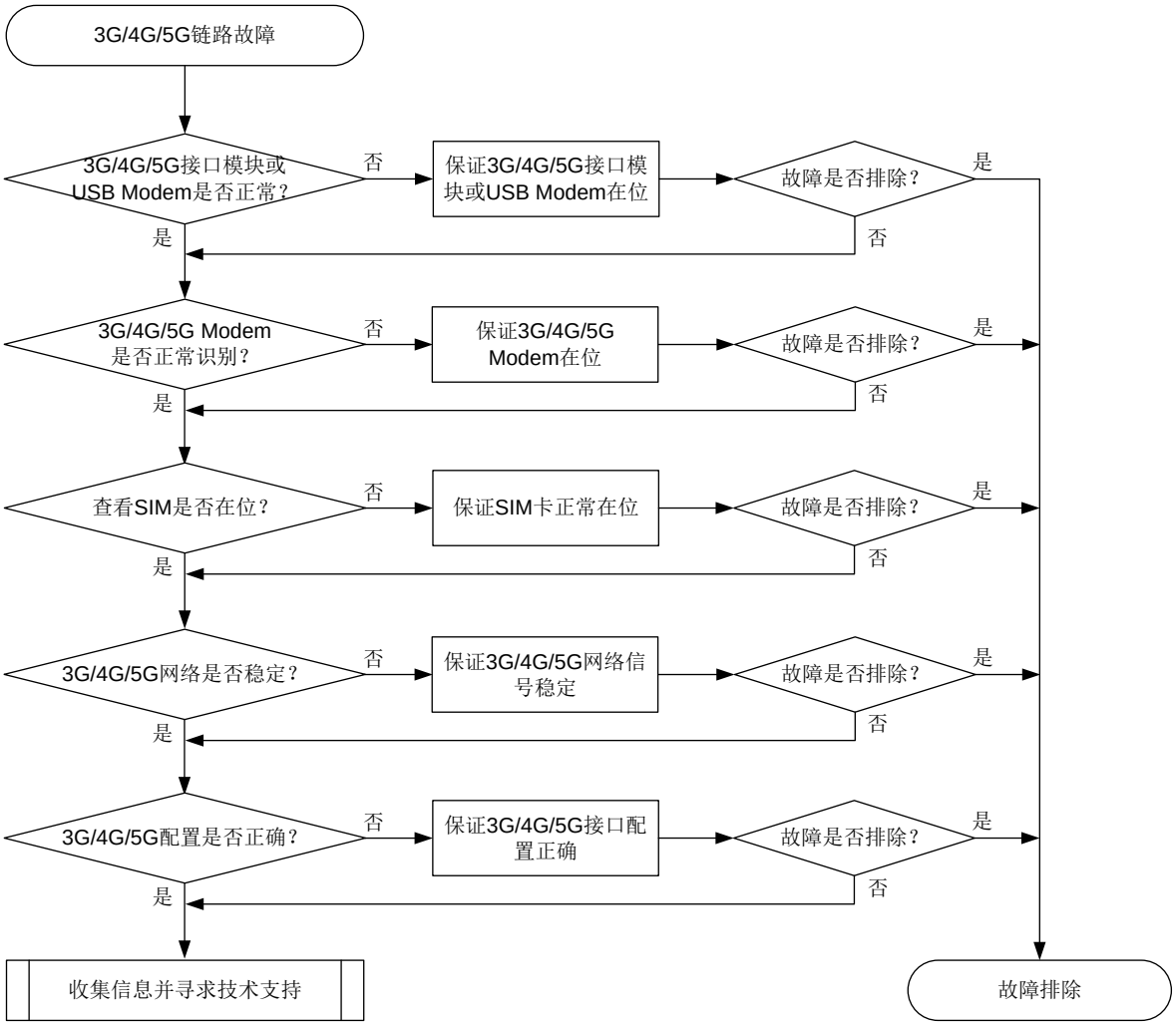
3.2 常见原因

- 3G/4G/5G 接口模块或者 USB 3G/4G Modem 型号和主机型号不匹配。
- 主机软件版本不支持使用该 3G/4G/5G 接口模块。
- 3G/4G/5G 接口模块安装的槽位不正确。
- 3G/4G/5G 接口模块未安装到位。
- 3G/4G/5G 接口模块热插拔操作不当。
- 3G/4G/5G 接口模块或者 USB 3G/4G Modem 故障。
- 3G/4G/5G Modem 未识别。
- SIM 卡状态异常。
- 3G/4G/5G 网络不稳定。
- 3G/4G/5G 接口配置不正确。

3.3 故障分析

本类故障的诊断流程如图 28 所示。

图28 3G/4G/5G 链路故障诊断流程图



3.4 处理步骤

3.4.1 检查 3G/4G/5G 接口模块或者 USB 3G/4G Modem 状态

(1) 检查 3G/4G/5G 接口模块上的指示灯，如果所有指示灯均熄灭，则执行 **display device** 和 **display device manuinfo** 命令，查看 Slot 和电子标签信息。

```
<Sysname> display device
 Slot No.     Board Type              Status          Max Ports
 ------------------------------------------------------------
 0             RPU                      Normal          30
 1             Unknown                  Abnormal        Unknown
<Sysname>display device manuinfo
...
```

```
 Slot 1:
DEVICE_NAME           : NONE
DEVICE_SERIAL_NUMBER  : NONE
MAC_ADDRESS           : NONE
MANUFACTURING_DATE    : NONE
VENDOR_NAME           : NONE
```

(2) 如果 Slot 状态显示为 Unknown，电子标签等相关信息显示为 NONE。确认接口模块的型号是否和主机型号匹配，以及接口模块安装在主机的槽位是否正确，具体请参见《H3C MSR 系列路由器 接口模块手册》；如果是 USB 3G/4G Modem，请联系技术支持确认主机是否支持该 Modem。

(3) 确认接口模块是否安装到位。若未安装好，请重新拔插一下接口模块。重新插入前务必检查接口模块的连接器状态，看连接器是否变形、脏污。

(4) 将接口模块放到别的槽位，或者将主机上别的正常的接口模块放到这个槽位，进一步确认是不是接口模块故障。

(5) 仅部分带有 REMOVE 按钮接口模块支持热插拔，但是需要通过操作 REMOVE 按钮后再拔出接口模块，操作不当会导致设备或接口模块异常。如果已经带电拔插过接口模块，请尝试给主机断电重启恢复。

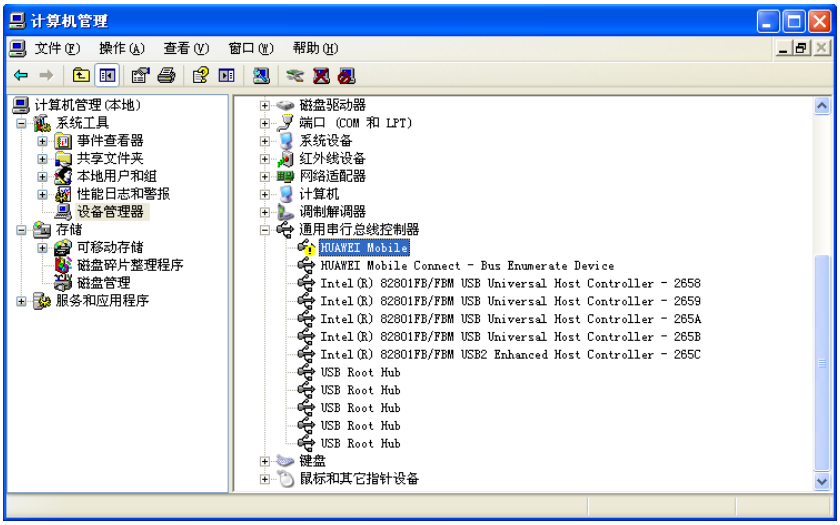
(6) 确认主机软件版本是否支持该接口模块。

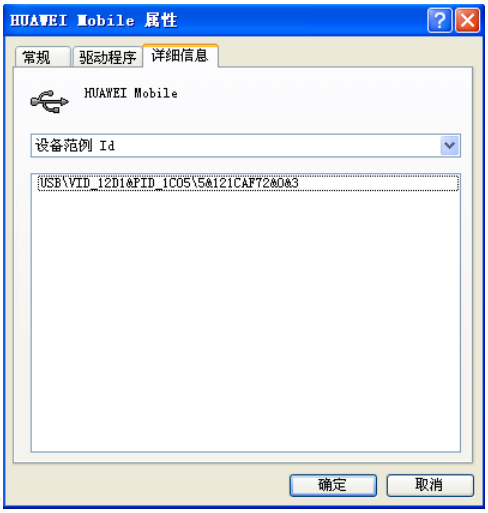
a. 通过 **display version** 命令查看主机软件版本；

b. 联系技术支持，确认当前主机软件版本是否支持该接口模块；

c. 如果当前软件版本不支持该接口模块，请升级到正确版本。

(7) 如果是 USB 3G/4G Modem，请把 Modem 插到 PC 上，待识别后查看以下信息，看 PC 是否能正常识别该 Modem。





3.4.2 检查 3G/4G/5G Modem 状态

(1) 如果 3G/4G/5G 接口模块的信息可以正常显示，但是无法显示 3G/4G/5G Modem 的信息。执行 **display cellular** 命令，无法显示 Cellular 接口信息。

```
<Sysname> display cellular 1/0
                  ^
 % Wrong parameter found at '^' position.
```

(2) 确认 MSR 路由器的款型和槽位是否正确。若不正确，请在支持的路由器的正确槽位上使用接口模块，具体请参见《H3C MSR 系列路由器 接口模块手册》。

(3) 确认接口模块是否外观有损伤、槽位的针脚是否有损伤。

(4) 确认是否已经通过 **remove** 命令或者“REMOVE”按钮将接口模块 remove 掉。部分带有 REMOVE 按钮的接口模块，若 REMOVE 指示灯熄灭，请重新拔插接口模块或者在用户视图下执行 **reboot** 命令重启接口模块。

(5) 确认接口模块是否在重启，接口模块完成初始化需要一定时间，请等待 1-2 分钟。

(6) 确认设备的版本是否正确。路由器版本需要升级到支持该 Modem 版本。若不正确，请升级版本。

(7) 部分 CDMA 制式的 3G Modem 不插 SIM 卡无法识别，请插入 SIM 卡后再测试。这些 3G Modem 也不支持 4G SIM 卡，所以插入 4G SIM 卡也无法识别。

(8) 仅部分带有 REMOVE 按钮接口模块支持热插拔，但是需要通过操作 REMOVE 按钮后再拔出接口模块，操作不当会导致设备或接口模块异常。如果已经带电拔插过接口模块，请尝试给主机断电重启恢复。

3.4.3 检查 SIM 卡状态

(1) 3G/4G/5G 接口模块和 3G/4G/5G Modem 的信息都可以正常显示，但无法拨号成功并获取 IP 地址。查看接口模块的 WWAN 指示灯，如果为常灭，表明无线广域网链路处于未连接状态。执行 **display ip interface brief**，通道化以太网接口没有获取 IP 地址。

```
<Sysname> display ip interface brief
*down: administratively down
```

```
(s): spoofing  (l): loopback
Interface Physical Protocol  IP address/Mask  VPN instance Description
E-Ch1/0:0 down      down       --                --              --
```

(2) 请确认 SIM 卡与 Modem 支持的制式是否匹配。比如 WCDMA 制式的 Modem 插中国电信（CDMA 运营商）SIM 卡就无法注册网络。

(3) 请确认 SIM 卡的状态是否正常，SIM 卡有“OK、Not Inserted、Locked、Unknown、Network Reject”等状态，执行 **display cellular** 命令查看 SIM 卡状态。

```
<Sysname> display cellular 1/0
...
    SIM Status: OK
...
```

- OK 表示正常，无需处理。
- Not Inserted 表示 SIM 安装异常，请检查 SIM 卡是否插好以及外观是否有损坏。

  SIM 卡的缺口方向一定要与卡槽的缺口方向对应上，SIM 卡芯片面朝下，保证 SIM 卡接触良好；也可以再找一台设备或手机 SIM 卡，做 SIM 卡交叉测试；如果也没有问题，建议升级设备为最新的软件版本。
- Locked 表示被锁定，请先解锁后再使用。若未完全锁定可以通过 PUK 码解锁，执行 **pin unlock** 命令进行解锁；若完全锁定则需要到营业厅解锁。

  ```
  <Sysname> system-view
  [Sysname] controller Cellular 1/0
  [Sysname-Cellular1/0]pin unlock 87654321 1234
  PIN will be unlocked and changed to “1234”. Continue? [Y/N]:y
  PIN has been unlocked and changed successfully.
  ```
- Unknown 表示状态未知。请尝试重新拔插 SIM 卡或执行 **modem reboot** 命令重启 Modem。

  ```
  <Sysname> system-view
  [Sysname] controller cellular 1/0
  [Sysname-Cellular1/0] modem reboot
  ```
- Network Reject 表示 SIM 卡被拒绝接入网络。该状态处理方式同 Locked 和 Unknown。

(4) 请确认 SIM 卡是否欠费。执行 **display cellular** 命令，查看 Modem 信息。如果“Current Service Status:Emergency”，打电话给营业厅确认。如果欠费再充值后，运营商开机了，重启一下 Modem 或者将该 SIM 卡插入手机看是否能上网。

```
<Sysname> display cellular 1/0
...
      Network Information:
    Current Service Status:Emergency
...
```

3.4.4 检查 3G/4G/5G 网络信号状态

(1) 如果 3G/4G/5G 接口模块和 3G/4G/5G Modem 的信息都可以正常显示，SIM 卡状态也是正常，请查看当前 3G/4G/5G 网络信号状态。3G/4G/5G 接口模块都提供有网络信号强度的指示灯，例如 5G 接口模块提供有 5G 指示灯，如果 5G 指示灯常灭，表示无信号；如果 5G 指示灯慢闪，表示 5G 信号弱。不同接口模块指示灯情况有差异，具体请参见《H3C MSR 系列路由器接口模块手册》。

(2) 如果不方便查看指示灯状态，也可以通过执行 **display cellular** 命令查看当前网络的信号强度。

- 3G Modem 可以使用 RSSI 表示信号强度，其值在-90dBm 以下表示信号非常差，可能会影响业务正常使用。

```
<Sysname> display cellular 1/0
...
 Radio Information:
  Current Band: ANY
Current RSSI: -51 dBm
```

- 4G Modem 除了查看 RSSI 外，还要查看 RSRP，RSRP 在-100dBm 以下表示信号非常差。

```
<Sysname> display cellular 1/0
...
  LTE related info:
    Current RSSI: -79 dBm
    Current RSRQ: -9 dB
    Current RSRP: -106 dBm
    Current SNR: 5 dB
```

- 5G Modem 查看 5G NR 的信号强度，RSRP 在-89dBm 以下表示信号较弱，一100dB 左右就可能无法驻入 5G。

```
<Sysname> display cellular 1/0
...
  Radio Information:
    Technology Preference: No preference specified (AUTO)
    Technology Selected: NR && LTE
    Configured LTE Band =
1,2,3,4,5,7,8,12,13,14,17,18,19,20,25,26,28,29,30,32,34,38,39,40,41,42,43
  5G availability under LTE system info:
    Current PCI: 537
    Endc Available: 1
    Restrict Dcnr: 0
    R15Availabe: 1
  NR related info:
    Current RSRQ: -12 dB
    Current RSRP: -93 dBm
    Current SNR: 14 dB
  LTE related info:
    Current RSSI: -65 dBm
    Current RSRQ: -13 dB
    Current RSRP: -103 dBm
    Current SNR: -2 dB
    Tx Power: 10 dBm
```

(3) 如果确认 3G/4G/5G 无信号，请先检查天线是否正常连接。

a. 设备内置模块和 SIC 卡必须安装外置天线，USB Modem 不需要。另外，3G Modem 可以只安装一根天线，但是天线必须安装到“MAIN”天线接口，不能接到“DIV”天线接口；4G Modem 必须安装 2 根天线；5G Modem 建议使用 4 根天线。

b. 如果天线连接正常，请继续确认周围是否有 3G/4G/5G 网络覆盖。可以使用手机或其他终端插 SIM 卡尝试，看是否能拨号成功。如果不行，请联系运营商解决。

(4) 如果确认 3G/4G/5G 信号比较弱，建议调整天线位置来增强无线信号。请注意，天线的方向一般要竖直向上，棒状天线之间可以呈八字状或剪刀状错开。在室内信号比较弱的地方，也可以通过增加天线延长线方式来增强无线信号。

3.4.5 检查 3G/4G/5G 接口的配置

(1) 如果 3G/4G/5G 接口模块的各项指示灯显示正常，但是 3G/4G/5G 链路仍然无法正常工作，此时，可以检查下 3G/4G/5G Cellular 接口的配置是否正确。3G/4G/5G Cellular 接口的配置，请参见配套配置手册中“二层技术-广域网接入配置指导”内的“移动通信 Modem 管理配置”。一般建议配置永久在线模式，如果配置了按需拨号，需要流量才能触发拨号，ping 几个包试试 Eth-channel 接口是否能够 UP。

(2) 如果是 USB 4G Modem，由于 USB 4G Modem 模块不支持通过配置命令来管理 Modem 模块，具体配置请参考对应主机的 Web 配置指导手册。

(3) 如果是连接 VPDN 网络，需要向运营商咨询正确的 APN、用户名和密码。

- 对于 3G Modem，可以通过 **profile create** 命令设置 APN、用户名和密码。

```
<Sysname> system-view
[Sysname] controller cellular 1/0
[Sysname-Cellular1/0] profile create 1 static cmnet authentication-mode pap user abc
password abc
```

- 对于 4G/5G Modem，可以通过 **apn-profile** 命令设置 APN、用户名和密码。

```
[Sysname] apn-profile test
[Sysname-apn-profile-test]apn static 3gnet
[Sysname-apn-profile-test]authentication-mode chap user card password simple card
```

(4) 请检查是否配置了当前运营商 SIM 卡不支持的 band。band 是用来配置模块工作的频段，各运营商 SIM 卡支持的 band 都不相同，一般缺省配置多个 band 来同时支持这些频段。如果该 SIM 卡支持的 band 不在这些缺省配置的 band 中或者配置限定到某些 band，但是该 SIM 卡不支持，就会导致拨号失败。所以，如无必要，无需修改 band 配置，如果因为已配置了不支持的 band 而导致拨号失败，可以通过删除 band 配置来恢复。

(5) 如果 Modem 配置了 IMSI 绑定，但配置的 IMSI 号和实际使用的 SIM 卡 IMSI 不一致，会导致拨号失败。可以通过执行 **display cellular** 命令查看 SIM 卡的 IMSI 串号。

```
<sysname>display cellular 1/0
Cellular1/0:
 Modem State:
  Hardware Information:
    Model: RM500QGL_VH
    Manufacturer: QUALCOMM INCORPORATED
    Modem Firmware Version: RM500QGLABR01A01M4G
    International Mobile Equipment Identity (IMEI): 863305040121609
    International Mobile Subscriber Identity (IMSI): 460028012255957
    Hardware Version: 20000
    Modem Status: Online
    Modem Status: IPv4 Active.
...
```

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

3.5 告警与日志

相关告警

无

相关日志

无

4 基础配置类故障处理

4.1 登录设备类故障处理

4.1.1 Console 口密码遗忘

1. 故障描述

Console 口采用 Password 认证或 AAA 本地认证的情况下，管理员通过 Console 口登录设备时，因密码不正确而无法成功登录。

2. 常见原因

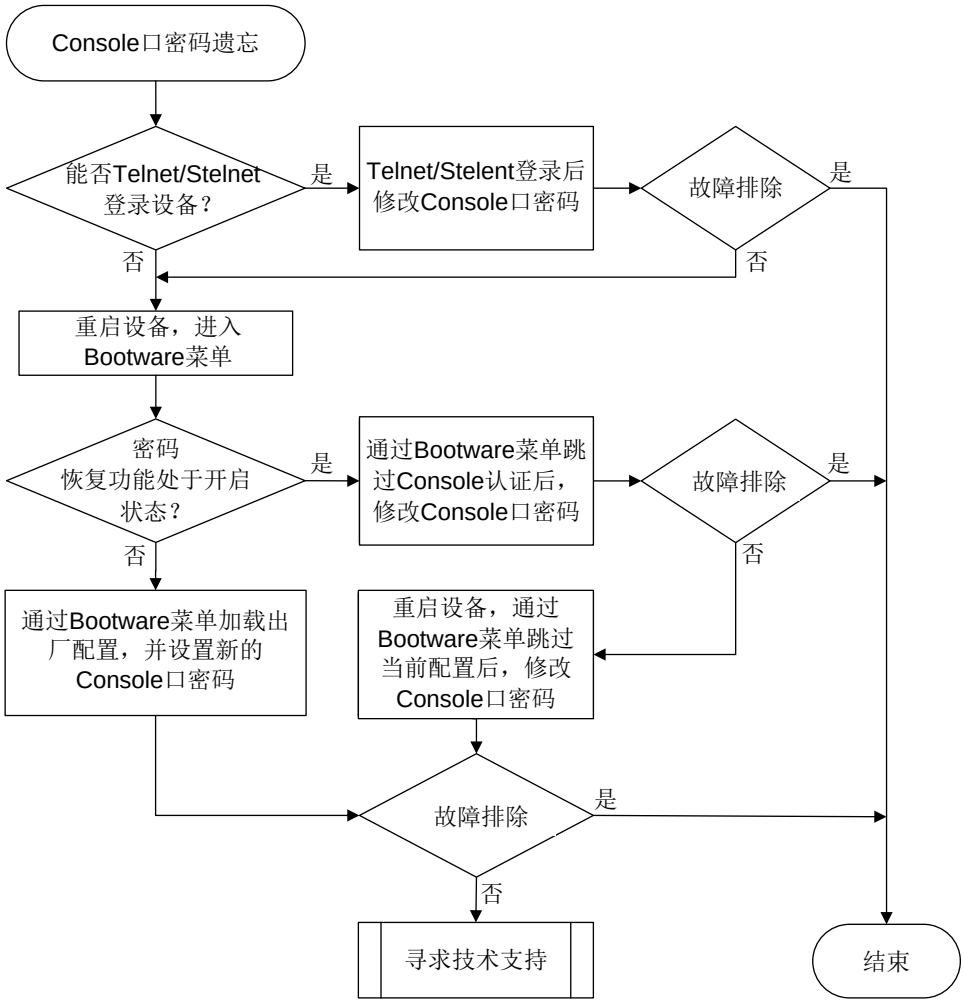
本类故障的常见原因主要包括：

- 管理员遗忘了 Console 口的登录密码或输入错误的密码。
- Console 口的登录账户已过期。

3. 故障分析

本类故障的诊断流程如图 29 所示。

图29 Console 口密码遗忘故障诊断流程图



4. 处理步骤

(1) 确认是否能过通过 Telnet/Stelnet 方式登录设备。

如果管理员拥有 Telnet/Stelnet 账号，并且该账号拥有 network-admin/level-15 用户角色，则可以通过 Telnet/Stelnet 方式登录到设备后修改 Console 口登录相关配置。具体的处理步骤如下：

a. 使用 Telnet/Stelnet 账号登录设备，执行 **display line** 命令查看 Console 口所在用户线的认证方式。

```
<Sysname> display line
  Idx  Type     Tx/Rx      Modem Auth  Int          Location
  0    CON 0    9600       -     P     -            0/0
+ 81   VTY 0               -     N     -            0/0
...
```

以上显示信息中，“Auth”字段取值为 P 表示采用密码认证方式，取值为 A 表示采用 AAA 认证方式。

b. 确认当前登录的 Telnet/Stelnet 用户是否具有 network-admin/level-15 用户角色。

对于采用 none 或者 password 认证方式登录的用户，可在当前登录的用户线视图下查看用户角色配置是否为 network-admin/level-15；对于采用 scheme 认证方式登录的用户，用户角色由 AAA 授权，需要查看对应的本地账号或远程账号的授权用户角色属性。

```
<Sysname> system-view
[Sysname-line-vty0] display this
#
line con 0
 authentication-mode password
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
#
return
```

如果用户角色不是 network-admin/level-15，则当前登录的账户没有更改 Console 口相关配置的权限，请执行步骤（2）；如果用户角色为 network-admin/level-15，请根据 Console 口的认证方式采用不同的处理步骤。

c. Console 口采用密码认证方式的情况下，修改 Console 口认证密码。

进入 Console 口所在的用户线，设置新的密码（下例中为 1234567890!）。同时，建议将用户角色设置为 network-admin/level-15，避免 Console 口登录后用户权限过低。

```
[Sysname] line console 0
[Sysname-line-console0] set authentication password simple 1234567890!
[Sysname-line-console0] user-role network-admin
```

d. Console 口采用 AAA 本地认证方式的情况下，修改 Console 口的本地用户密码。

进入 Console 口登录所使用账户的本地用户视图，修改本地用户的密码（下例中用户名为 admin，用户密码为 1234567890!）。同时，建议将用户角色设置为 network-admin/level-15，避免 Console 口登录后用户权限过低。

```
[Sysname] local-user admin class manage
[Sysname-luser-manage-admin] password simple 1234567890!
[Sysname-luser-manage-admin] authorization-attribute user-role network-admin
```

e. Console 口采用 AAA 远程认证方式的情况下，请联系 AAA 服务器管理员获取登录密码。

f. 为了防止重启后配置丢失，请执行 **save** 命令保存当前配置。

(2) 通过 Console 口连接设备后，断电重启设备，进入 BootWare 菜单。

说明

- 进入到 BootWare 菜单需要重启设备，会导致业务中断，请视具体情况做好备份，并尽量选择业务量较少的时间操作。

系统启动后，如果未及时选择进入基本段，则会直接运行 BootWare 扩展段程序。当显示信息出现“Press Ctrl+B to access EXTENDED-BOOTWARE MENU...”时，键入<Ctrl+B>，系统会首先给出密码恢复功能是否开启的提示信息：

```
Password recovery capability is enabled.
Password recovery capability is disabled.
```

- 密码恢复功能处于开启状态时，可以选择跳过 Console 口认证选项，或者跳过当前配置选项。具体操作过程请分别参见步骤（3）、（4）。
- 密码恢复功能处于关闭状态时，可以选择恢复出厂配置选项。具体操作过程请执行步骤（5）。

(3) 通过 BootWare 扩展段菜单跳过 Console 口认证，登录后修改 Console 口密码。

直接回车，进入 BootWare 扩展段主菜单后，请按照系统提示选择相应的菜单选项跳过 Console 口认证（不同产品跳过 Console 口认证的菜单选项不同，请以实际情况为准）。系统启动后，不需要管理员输入 Console 口密码，会正常完成所有配置的加载。

a. 启动后，请尽快根据 Console 口采用的认证方式修改密码。

   – Console 口采用密码认证方式的情况下，修改 Console 口认证密码。

   进入 Console 口所在的用户线，设置新的密码（下例中为 1234567890!）。同时，建议将用户角色设置为 network-admin/level-15，避免 Console 口登录后用户权限过低。

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] set authentication password simple 1234567890!
[Sysname-line-console0] user-role network-admin
```

   – Console 口采用 AAA 本地认证方式的情况下，修改 Console 口的本地用户密码。

   进入 Console 口登录所使用账户的本地用户视图，修改本地用户的密码（下例中用户名为 admin，用户密码为 1234567890!）。同时，建议将用户角色设置为 network-admin/level-15，避免 Console 口登录后用户权限过低。

```
<Sysname> system-view
[Sysname] local-user admin class manage
[Sysname-luser-manage-admin] password simple 1234567890!
[Sysname-luser-manage-admin] authorization-attribute user-role network-admin
```

b. 为了防止重启后配置丢失，请执行 **save** 命令保存当前配置。

(4) 通过 BootWare 扩展段菜单跳过当前配置，登录后配置新的 Console 口密码。

直接回车，进入 BootWare 扩展段主菜单后，请按照系统提示选择相应的菜单选项跳过当前配置（不同产品跳过当前配置的菜单选项不同，请以实际情况为准）。系统启动时，将忽略配置文件中的所有配置以空配置进行启动（该选项每次设置后仅生效一次）。系统启动后，不需要管理员输入 Console 口密码。

a. 启动后，请尽快将原配置文件导出。在此操作过程中不要对设备进行断电。

   – 方式一：通过 FTP/TFTP 方式将原配置文件导出到本地。

   – 方式二：在用户视图下执行 **more** 命令查看原配置文件内容，将显示的所有原配置文件内容直接复制粘贴到本地文件中。

b. 手动修改本地配置文件中关于 Console 口登录的配置，将修改后的配置文件上传至设备存储介质的根目录下。

c. 配置下次启动时的配置文件为修改后的配置文件（假设修改后的配置文件为 startup.cfg）。

```
<Sysname> startup saved-configuration startup.cfg
```

d. 重启设备。

(5) 通过 BootWare 扩展段菜单恢复出厂配置，登录后配置新的 Console 口密码。

说明

此操作下，系统启动时会自动删除下次启动配置文件和备份启动配置文件，再以出厂配置启动。请确保当前业务不会受到影响时执行本操作。

直接回车，进入 BootWare 扩展段主菜单后，请按照系统提示选择相应的子菜单恢复出厂配置（不同产品恢复出厂配置的菜单选项不同，请以实际情况为准）。系统启动后，不需要管理员输入 Console 口密码。

a. 启动后，请根据实际需要配置 Console 口的登录认证方式，以及相关的登录密码或登录账户。

   – 认证方式为 **none**

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] authentication-mode none
[Sysname-line-console0] user-role network-admin
```

   该方式下，用户不需要输入用户名和密码，就可以使用该用户线登录设备，存在安全隐患，请谨慎配置。

   – 认证方式为密码认证

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] authentication-mode password
[Sysname-line-console0] set authentication password simple 1234567890!
[Sysname-line-console0] user-role network-admin
```

   – 认证方式为本地 AAA 认证

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] authentication-mode scheme
[Sysname-line-console0] quit
[Sysname] local-user admin class manage
[Sysname-luser-manage-admin] service-type terminal
[Sysname-luser-manage-admin] password simple 1234567890!
[Sysname-luser-manage-admin] authorization-attribute user-role network-admin
```

   – 认证方式为远程 AAA 认证

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] authentication-mode scheme
[Sysname-line-console0] quit
```

   除此之外，还需要配置 Login 用户的认证域，以及 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

b. 为了防止重启后配置丢失，请执行 **save** 命令保存当前配置。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

4.1.2 Telnet 登录密码遗忘

1. 故障描述

设备对 Telnet 登录用户采用 Password 认证或 AAA 本地认证的情况下，管理员遗忘 Telnet 账户密码无法登录设备。

2. 常见原因

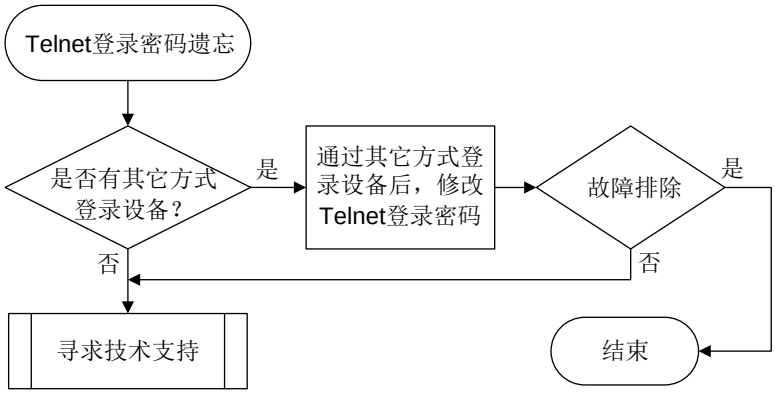
本类故障的常见原因主要包括：

- 管理员遗忘了 Telnet 口的登录密码或输入错误的密码。
- Telnet 登录账户已过期。

3. 故障分析

本类故障的诊断流程如图 30 所示。

图30 Telnet 登录密码遗忘故障诊断流程图



4. 处理步骤

(1) 确认是否有其它方式可以登录设备。

如果 Telnet 登录密码丢失，可以通过其他方式（例如 Console 口）登录设备后重新进行配置。

a. 使用其它方式登录设备，执行 **display line** 命令查看 VTY 口所在用户线的认证方式。

```
<Sysname> display line
  Idx  Type     Tx/Rx      Modem Auth  Int          Location
+ 0    CON 0    9600       -     P     -            0/0
  81   VTY 0               -     P     -            0/0
...
```

以上显示信息中，“Auth”字段取值为 P 表示采用密码认证方式，取值为 A 表示采用 AAA 认证方式。

b. 根据 VTY 口的认证方式，采用不同的处理步骤重新设置新的登录密码。

– 采用密码认证

设置 VTY 登录用户的认证方式为密码认证，假设登录密码为 1234567890!，用户角色为 network-admin。

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode password
[Sysname-line-vty0-63] set authentication password simple 1234567890!
[Sysname-line-vty0-63] user-role network-admin
```

– 采用 AAA 本地认证

设置 VTY 登录用户的认证方式为 AAA 认证，假设登录使用的本地账户名为 admin，使用的本地密码为 1234567890!，用户角色为 network-admin。

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
[Sysname] local-user admin class manage
[Sysname-luser-manage-admin] service-type telnet
[Sysname-luser-manage-admin] password simple 1234567890!
[Sysname-luser-manage-admin] authorization-attribute user-role network-admin
```

如果忘记原有登录账户名，可参考以上步骤创建新的本地账户。

– 采用 AAA 远程认证

该认证方式下，请联系 AAA 服务器管理员获取登录密码。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

5 设备管理类故障处理

5.1 硬件资源管理故障处理

5.1.1 CPU 占用率高

1. 故障描述

当出现以下情况时，说明设备的 CPU 控制核占用率高，需要确认 CPU 占用率高的具体原因。

- 对设备进行每日巡检时，连续使用 **display cpu-usage** 命令查看 CPU 的占用率，CPU 占用率明显比日常平均值高。

执行 **display cpu-usage summary** 命令显示最近 5 秒、1 分钟、5 分钟内 CPU 占用率的平均值。

```
<Sysname> display cpu-usage summary
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          5%                5%                4%
```

执行 **display cpu-usage history** 命令以图表的方式显示最近 60 个采样点的 CPU 占用率，观察到 CPU 占用率持续在增长或者明显比日常平均值高。

- 通过 Telnet/SSH 等方式登录设备，并执行命令行时，设备反应缓慢，出现卡顿现象。
- 设备上打印 CPU 占用率高的相关日志。
- SNMP 网管上出现 CPU 占用率高的相关告警。

2. 常见原因

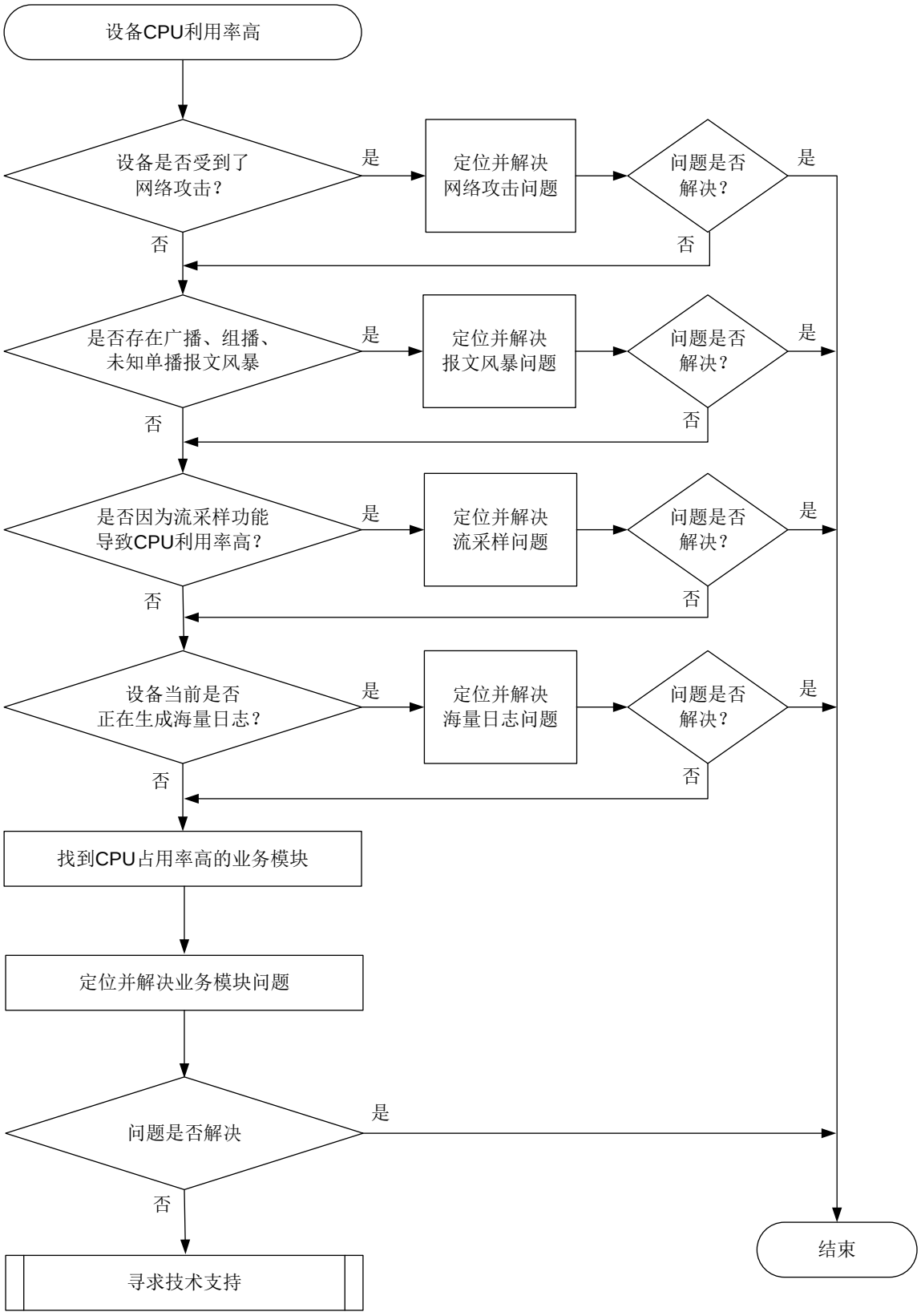
本类故障的常见原因主要包括：

- 网络攻击。
- 协议震荡，通常为 STP 震荡、路由协议震荡等。
- 网络环路。
- 设备上配置了流采样功能，需要处理的流量太大或者设备采样频率太高，导致采样功能占用大量 CPU 资源。
- 设备产生海量日志，设备生成和管理这些日志需要占用大量 CPU 资源。

3. 故障分析

本类故障的诊断流程如图 31 所示。

图31 CPU 占用率高的故障诊断流程图



4. 处理步骤

(1) 确认设备是否受到网络攻击。

现网中，导致设备 CPU 占用率高最常见的原因是网络攻击。攻击者发起大量非正常网络交互对设备产生冲击，例如短时间内发送大量 TCP 连接建立请求报文或者 ICMP 请求报文，设备忙于处理这些攻击报文，导致 CPU 占用率高，从而影响设备正常业务的运行。

Probe 视图下执行 **display system internal control-plane statistics** 命令，查看控制平面报文的统计信息，关注丢弃报文的数量。如果当前 CPU 占用率高，且 Dropped 字段取值较大，则设备大概率受到了报文攻击。

```
<Sysname> display system internal control-plane statistics slot 1
Control plane slot 1
  Protocol: Default
    Bandwidth: 15360 (pps)
    Forwarded: 108926 (Packets), 29780155 (Bytes)
    Dropped  : 0 (Packets), 0 (Bytes)
  Protocol: ARP
    Bandwidth: 512 (pps)
    Forwarded: 1489284 (Packets), 55318920 (Bytes)
    Dropped  : 122114 (Packets), 491421 (Bytes)
...
```

- 如果受到了网络攻击，则先解决网络攻击问题。
- 如果未受到网络攻击，则执行步骤(2)。

(2) 确认设备是否出现协议震荡。

协议震荡会导致设备不断地处理协议报文、计算拓扑、更新表项，引起 CPU 占用率高。在实际应用中，最常见的协议震荡为 STP 协议震荡和 OSPF 协议震荡。

- 对于 STP 协议震荡，在系统视图执行 **stp port-log** 命令打开端口状态变化日志显示开关，如果命令行界面频繁输出以下日志，则说明出现了 STP 协议震荡。

  ```
  STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.
  STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/0/1 has been set to discarding state.
  STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/0/1 was notified a topology change.
  ```

  - 如果 STP 协议震荡，请先排除 STP 协议震荡问题。
  - 如果 STP 协议没有震荡，则继续定位。
- 对于 OSPF 协议震荡，执行 **display ip routing-table** 命令，查看路由信息。如果路由表项中相同网段的路由条目被频繁反复地创建和删除，则表示路由震荡。
  - 如果路由震荡，或者路由一直不存在，则先排除链路问题和 IGP 路由问题。
  - 如果路由没有震荡，则执行步骤(3)。

(3) 确认是否存在网络环路。

当以太网接口工作在二层模式并且链路存在环路时，可能出现广播风暴和网络振荡。大量的协议报文上送 CPU 处理，从而导致 CPU 占用率升高。当存在网络环路时，设备很多端口的流量会明显变大，且广播和组播报文占比较大。可通过以下步骤来确认设备是否存在网络环路，设备是否存在广播、组播、未知单播报文风暴。

a. 清除接口的统计信息。

```
<Sysname> reset counters interface
```

b. 多次执行 **display counters rate inbound interface** 命令查看端口使用率是否明显增大。

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface               Usage(%)     Total(pps) Broadcast(pps) Multicast(pps)
GE5/3/0                     0.01              7            --             --
MGE0/31/0                   0.01              1            --             --
MGE0/32/0                   0.01              5            --             --
VMC1/1/0                    0.05             60            --             --
VMC1/2/0                    0.04             52            --             --

 Overflow: More than 14 digits.
       --: Not supported.
```

c. 如果端口使用率明显增大，可继续多次执行 **display counters inbound interface** 命令查看接口收到的总报文数、广播和组播报文的数量，分别对应显示信息中 Total(pkt)、Broadcast(pkt)、Multicast(pkt)字段的取值。如果广播和组播报文的增长速度快，广播、组播报文在接口收到的总报文数中占比大，则可能出现广播/组播风暴。如果广播和组播报文数量没有明显增加，但是接口收到的总报文数明显增加，则可能出现未知单播报文风暴。

```
<Sysname> display counters inbound interface
Interface                 Total(pkt) Broadcast(pkt) Multicast(pkt) Err(pkt)
GE5/3/0                          141            27            111        0
MGE0/31/0                     274866         47696              0       --
MGE0/32/0                    1063034        684808              2       --
VMC1/1/0                    11157797       7274558             50        0
VMC1/2/0                     9653898       5619640             52        0

 Overflow: More than 14 digits (7 digits for column "Err").
       --: Not supported.
```

- 如链路出现环路，可进行如下处理：
  - 排查链路连接，避免物理拓扑出现环路。
  - 使用 **display stp** 命令检查 STP 协议是否使能，配置是否正确。如果配置错误，请修改配置。
  - 使用 **display stp brief** 和 **display stp abnormal-port** 命令检查邻接设备 STP 状态是否正常。请根据 **display stp abnormal-port** 命令显示信息中的 BlockReason 字段的取值，定位并解决 STP 异常问题。

    如 STP 配置均正确，可能为 STP 协议计算错误或协议计算正确但端口驱动层没有正常 Block 阻塞，可以在发生环路的接口上执行 **shutdown**/**undo shutdown** 命令或者拔插网线让 STP 重新计算来快速恢复 STP 功能，消除环路。
  - 在以太网接口视图下，使用 **broadcast-suppression** 命令开启端口广播风暴抑制功能，使用 **multicast-suppression** 命令开启端口组播风暴抑制功能，使用 **unicast-suppression** 命令开启端口未知单播风暴抑制功能。或者使用 **flow-control** 命令配置流量控制功能。

- 使用 QoS 策略针对组播、广播和未知单播报文进行限速。

- 如未出现环，请执行步骤(4)。

(4) 确认是否配置了流统计和采样功能，以及配置的参数是否合适。

当设备上配置了 NetStream、sFlow 等网络流量监控功能后，设备会对网络流量进行统计分析。如果网络流量较高，可能会导致 CPU 占用率偏高。此时，可进行以下处理：

- 配置过滤条件来精确匹配流量，仅统计分析用户关心的流量。
- 配置采样器，调整采样比例，使得 NetStream、sFlow 收集到的统计信息既能基本反映整个网络的状况，又能避免统计报文过多影响设备转发性能。

(5) 确认设备当前是否正在生成海量日志。

某些异常情况下，例如，设备受到攻击、运行中发生了错误、端口频繁 Up/Down 等，设备会不停地产生诊断信息或日志信息。此时系统软件要频繁的读写存储器，会造成 CPU 占用率升高。

可通过以下方式来判断设备是否正在生成海量日志：

- Telnet 登录到设备，配置 **terminal monitor** 命令允许日志信息输出到当前终端。

```
<Sysname> terminal monitor
The current terminal is enabled to display logs.
```

配置该命令后，如果有大量异常日志或者重复日志输出到命令行界面，则说明设备正在生成海量日志。

- 重复执行 **display logbuffer summary** 命令，如果日志信息总量有明显的增加，再使用 **display logbuffer reverse** 命令查看日志详情，确认是否有大量异常日志或者某一条信息大量重复出现。

```
<Sysname> display logbuffer summary
  Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     1     0     0     2     9    24    12   128     0
     5     0     0     0    41    72     8     2     0
    97     0     0    42    11    14     7    40     0
<Sysname> display logbuffer reverse
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 410
%Jan 15 08:17:24:259 2021 Sysname SHELL/6/SHELL_CMD:
-Line=vty0-IPAddr=192.168.2.108-User=**; Command is display logbuffer
%Jan 15 08:17:19:743 2021 Sysname SHELL/4/SHELL_CMD_MATCHFAIL:
-User=**-IPAddr=192.168.2.108; Command display logfile in view shell failed to be
matched.
...
```

如果设备正在生成海量日志，可以通过以下方法减少日志的生成：

- 关闭部分业务模块的日志输出功能。
- 使用 **info-center logging suppress** 命令禁止指定模块日志的输出。
- 使用 **info-center logging suppress duplicates** 命令开启重复日志抑制功能。

如果设备未生成海量日志，则执行步骤(6)。

(6) 收集 CPU 占用率相关信息，找到 CPU 占用率高的业务模块。

a. 确定对 CPU 占用率高的任务。

在设备上执行 **display process cpu** 命令查看一段时间内占用 CPU 最多的任务。下面以 slot 1 上的操作为例。

```
<Sysname> display process cpu slot 1
CPU utilization in 5 secs: 0.4%; 1 min: 0.2%; 5 mins: 0.2%
    JID      5Sec      1Min      5Min    Name
      1      0.0%      0.0%      0.0%    scmd
      2      5.5%      5.1%      5.0%    [kthreadd]
      3      0.0%      0.0%      0.0%    [ksoftirqd/0]
...
```

如果某个进程的 CPU 占用率高于 3%（经验值供参考），则需要针对该进程继续定位。

在设备上执行 **monitor process dumbtty** 命令实时查看进程在指定 CPU 上的占用率。下面以 slot 1 CPU 0 为例。

```
<Sysname> system-view
[Sysname] monitor process dumbtty slot 1 cpu 0
206 processes; 342 threads; 5134 fds
Thread states: 4 running, 338 sleeping, 0 stopped, 0 zombie
CPU0: 99.04% idle, 0.00% user, 0.96% kernel, 0.00% interrupt, 0.00% steal
CPU1: 98.06% idle, 0.00% user, 1.94% kernel, 0.00% interrupt, 0.00% steal
CPU2: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU3: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU4: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
Memory: 7940M total, 5273M available, page size 4K
        JID        PID  PRI State  FDs     MEM  HH:MM:SS    CPU   Name
        322        322  115   R     0       0K  01:48:03  20.02%  [kdrvfwdd2]
        323        323  115   R     0       0K  01:48:03  20.02%  [kdrvfwdd3]
        324        324  115   R     0       0K  01:48:03  20.02%  [kdrvfwdd4]
        376        376  120   S    22  159288K  00:00:07   0.37%  diagd
          1          1  120   S    18   30836K  00:00:02   0.18%  scmd
        379        379  120   S    22  173492K  00:00:11   0.18%  devd
          2          2  120   S     0       0K  00:00:00   0.00%  [kthreadd]
          3          3  120   S     0       0K  00:00:02   0.00%  [ksoftirqd/0]
...
```

– 在 **monitor process dumbtty** 命令显示信息中找到 CPU 占用率超过 3%（经验值供参考）的进程的 JID，再对这些进程执行 **display process job** 命令，收集进程的详细信息，并确认该进程是否运行在控制核上。

如果 **display process job** 命令的显示信息中 LAST_CPU 字段的取值为控制核的编号（例如 0～1），则说明该进程运行在 CPU 控制核上，则需要进一步定位；如果显示信息中 LAST_CPU 字段的取值为非控制核的编号，则说明该进程运行在 CPU 转发核上，无需关注，请执行步骤(7)。下面以 pppd 进程为例，通过显示信息可以看到，该进程包含多个线程，这些线程都运行在控制核上。

```
<Sysname> display process name pppd
                              Job ID: 515
                                 PID: 515
```

```
                        Parent JID: 1
                        Parent PID: 1
                   Executable path: /sbin/pppd
                          Instance: 0
                           Respawn: ON
                     Respawn count: 1
              Max. spawns per minute: 12
                      Last started: Wed Nov  3 09:52:00 2021
                     Process state: sleeping
                          Max. core: 1
                               ARGS: --MaxTotalLimit=2000000
--MaxIfLimit=65534 --CmdOption=0x01047fbf --bSaveRunDb --pppoechastenflag=1
--pppoechastennum=6 --pppoechastenperiod=60 --pppoechastenblocktime=300
--pppchastenflag=1 --pppchastennum=6 --pppchastenperiod=60
--pppchastenblocktime=300 --PppoeKChasten --bSoftRateLimit --RateLimitToken=2048
      TID  LAST_CPU    Stack      PRI    State   HH:MM:SS:MSEC  Name
      515      0        136K      115      S     0:0:0:90       pppd
      549      0        136K      115      S     0:0:0:0        ppp_misc
      557      0        136K      115      S     0:0:0:10       ppp_chasten
      610      0        136K      115      S     0:0:0:0        ppp_work0
      611      1        136K      115      S     0:0:0:0        ppp_work1
      612      1        136K      115      S     0:0:0:0        ppp_work2
      613      1        136K      115      S     0:0:0:0        mp_main
      618      1        136K      115      S     0:0:0:110      pppoes_main
      619      1        136K      115      S     0:0:0:100      pppoes_mesh
      620      1        136K      115      S     0:0:0:120      l2tp_mesh
      621      1        136K      115      S     0:0:0:20       l2tp_main
```

– 对于运行在控制核、CPU 占用率超过 5%的进程，查看进程的 Name 字段的取值来确定该进程是否为用户态进程。

  如果 Process 的 Name 取值中包含“[]”，表示它是内核线程，无需执行 **monitor thread dumbtty** 命令；如果 Process 的 Name 取值中未包含“[]”，表示它是用户态进程，它可能包含多个线程。对于多线程的用户态进程，还需要对该用户态进程执行 **monitor thread dumbtty** 命令，如果显示信息中某线程 LAST_CPU 字段的取值为 CPU 控制核的编号，且 CPU 字段取值大于 5%，则该线程可能为导致 CPU 控制核占用率高的线程，需要进一步定位。

```
<Sysname> monitor thread dumbtty slot 1 cpu 0
206 processes; 342 threads; 5134 fds
Thread states: 4 running, 338 sleeping, 0 stopped, 0 zombie
CPU0: 98.06% idle, 0.97% user, 0.97% kernel, 0.00% interrupt, 0.00% steal
CPU1: 97.12% idle, 0.96% user, 0.96% kernel, 0.96% interrupt, 0.00% steal
CPU2: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU3: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU4: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
Memory: 7940M total, 5315M available, page size 4K
        JID      TID  LAST_CPU  PRI  State  HH:MM:SS MAX   CPU     Name
        322      322      2     115    R    00:04:21    0  20.15%  [kdrvfwdd2]
        323      323      3     115    R    00:04:21    0  20.15%  [kdrvfwdd3]
        324      324      4     115    R    00:04:21    0  20.15%  [kdrvfwdd4]
```

```
             1         1     1     120     S   00:00:02   21   0.19%   scmd
           376       376     1     120     S   00:00:00    1   0.19%   diagd
             2         2     0     120     S   00:00:00    0   0.00%   [kthreadd]
  ...
```

b. 确认异常任务的调用栈。

在 Probe 视图下执行 **follow job** 命令确认异常任务的调用栈。下面以 Sysname 上（slot 1）pppd 进程（进程编号为 515）的操作为例。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe] follow job 515 slot 1
Attaching to process 515 (pppd)
Iteration 1 of 5
------------------------------
Thread LWP 515:
Switches: 3205
User stack:
#0  0x00007fdc2a3aaa8c in epoll_wait+0x14/0x2e
#1  0x0000000000441745 in ppp_EpollSched+0x35/0x5c
#2  0x0000000000000004 in ??
Kernel stack:
[<ffffffff811f0573>] ep_poll+0x2f3/0x370
[<ffffffff811f06c0>] SyS_epoll_wait+0xd0/0xe0
[<ffffffff814aed79>] system_call_fastpath+0x16/0x1b
[<ffffffffffffffff>] 0xffffffffffffffff
Thread LWP 549:
Switches: 20
User stack:
#0  0x00007fdc2a3aaa8c in epoll_wait+0x14/0x2e
#1  0x00000000004435d4 in ppp_misc_EpollSched+0x44/0x6c
Kernel stack:
[<ffffffffffffffff>] 0xffffffffffffffff
...
```

c. 根据 a 和 b 步骤找到任务名称，再根据任务名称找到对应的业务模块，定位并处理业务模块的问题。例如，如果任务 snmpd 的 CPU 占用率较高，可能是因为设备受到了 SNMP 攻击，或者 NMS 对设备的访问太频繁。需要进一步定位 SNMP 业务模块的问题；如果任务 nqad 的 CPU 占用率较高，可能是因为 NQA 探测太频繁，需要进一步定位 NQA 业务模块的问题。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

- hh3cEntityExtCpuUsageThresholdNotfication
- hh3cEntityExtCpuUsageThresholdRecover

- hh3cCpuUsageSevereNotification
- hh3cCpuUsageSevereRecoverNotification
- hh3cCpuUsageMinorNotification
- hh3cCpuUsageMinorRecoverNotification

相关日志

- DIAG/5/CPU_MINOR_RECOVERY
- DIAG/4/CPU_MINOR_THRESHOLD
- DIAG/5/CPU_SEVERE_RECOVERY
- DIAG/3/CPU_SEVERE_THRESHOLD

6 虚拟化技术类故障处理

6.1 IRF

6.1.1 IRF 组建失败

1. 故障描述

多台设备无法组建 IRF，或者新设备无法加入现有的 IRF。

2. 常见原因

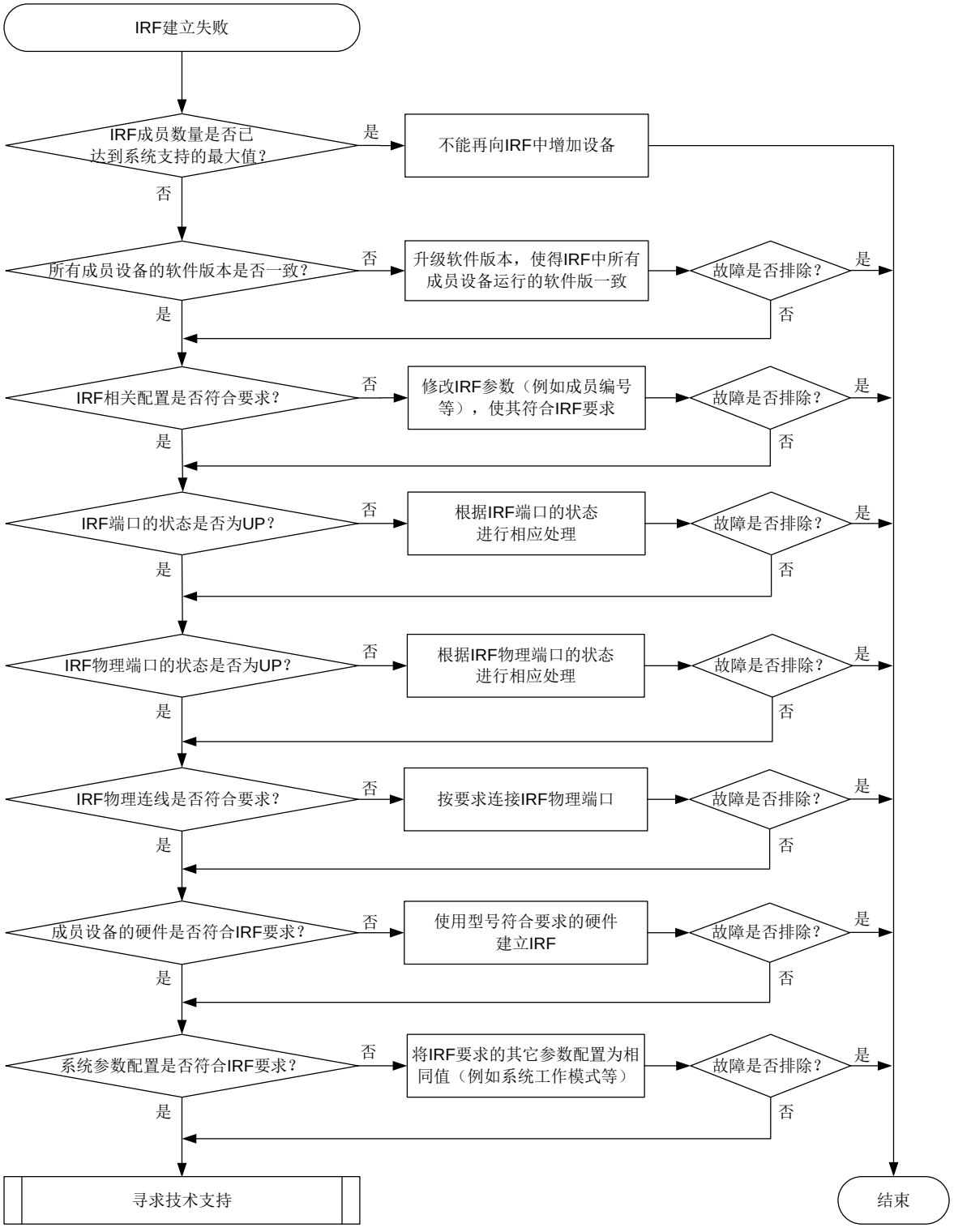
本类故障的常见原因主要包括：

- IRF 成员设备数量超出了产品支持的规格，导致新设备无法加入现有的 IRF。
- 配置不符合 IRF 要求，导致无法组建 IRF，或者新设备无法加入现有的 IRF。
- IRF 物理端口、线缆和物理拓扑不符合 IRF 要求，导致 IRF 链路无法达到 up 状态。

3. 故障分析

本类故障的诊断流程如图 32 所示。

图32 IRF 组建失败故障诊断流程图



4. 处理步骤

注意

本文仅列出组建 IRF 的常规要求，以供参考。组建 IRF 的完整要求请参见产品配套的《IRF 配置指导》。

(1) 检查 IRF 成员数量是否已达到系统支持的最大值。

请使用 **display irf** 命令查看当前 IRF 中的成员设备数量。如果 IRF 成员数量已经达到系统支持的最大值，则不允许再加入成员设备。

(2) 检查各成员设备使用的软件版本是否一致。

使用 **display version** 命令查看每台设备当前运行的软件版本，只有使用相同软件版本的设备才能组成 IRF。

IRF 系统启动文件自动加载功能（缺省为开启状态）可以自动将成员设备的软件版本与 IRF 中主设备进行同步，但是在成员设备与主设备的软件版本差异过大时，自动升级可能无法成功执行。此时，需要分别升级每台成员设备，使得所有成员设备的软件版本一致，之后再组建 IRF。

(3) 检查 IRF 的配置是否满足相关要求。

a. 确保设备运行在 IRF 模式。

部分产品出厂即为 IRF 模式，且不支持模式切换；部分产品出厂为独立运行模式，支持模式切换。如果设备当前支持 **display irf link** 或者 **display irf topology** 命令，则说明设备运行在 IRF 模式。否则，设备运行在独立运行模式，需要先在系统视图执行 **chassis convert mode irf** 命令将设备切换到 IRF 模式。

```
<Sysname> display irf ?
  >              Redirect it to a file
  >>             Redirect it to a file in append mode
  configuration  IRF configuration that will be valid after reboot
  link           Display link status
  topology       Topology information
  |              Matching output
  <cr>
```

b. 确保设备的成员编号在 IRF 中唯一。

请使用 **display irf** 命令查看 IRF 中各成员设备的成员编号。IRF 中各成员设备必须使用不同的编号，编号相同的设备不能建立或加入 IRF。设备缺省成员编号为 1，在独立运行模式下可通过 **irf member** 命令修改，在 IRF 模式下可通过 **irf member renumber** 命令修改。修改后需要保存配置并重启该设备，新编号才能生效。

c. 确保各成员设备的出厂桥 MAC 地址不同

具有相同出厂桥 MAC 的成员设备之间不能组成 IRF。通常情况下，设备出厂会携带全网唯一的桥 MAC 地址。如果 IRF 组建失败，且输出了日志信息“Failed to stack because of the same bridge MAC addresses.”，则表明两台设备的出厂桥 MAC 相同，可在其中一台设备上执行 **irf mac-address** 命令修改桥 MAC。（**irf mac-address** 命令的支持情况与设备的型号有关，请以设备的实际情况为准）

d. 确保同一 IRF 系统中所有成员设备的 IRF 域编号一致。

IRF 域编号不影响 IRF 的组建和合并，但是会影响 MAD 检测。为了使 MAD 功能正常工作，请确保同一 IRF 系统中所有成员设备的 IRF 域编号一致。IRF 域编号缺省值为 0。在单台设备上执行 **display irf** 命令，可通过显示信息中的 Domain ID 字段查看 IRF 域编号。如果设备的 IRF 域编号和其它设备不同，可在该设备上执行 **irf domain** 命令修改。

(4) 检查 IRF 端口的状态，使其变成 UP 状态。

IRF 端口是一种专用于 IRF 连接的逻辑接口，需要与物理端口绑定后才能生效。请通过 **display irf topology** 命令显示信息的 Link 字段来确认 IRF 端口的状态。

```
<Sysname> display irf topology
                              Topology Info
-------------------------------------------------------------------------
               IRF-Port1                IRF-Port2
MemberID    Link       neighbor      Link       neighbor    Belong To
2           DIS        ---           UP         1           5e40-08d9-0104
1           UP         2             DIS        ---         5e40-08d9-0104
```

- 如果 Link 字段取值为 UP，则表示 IRF 端口连接正常，无需处理。
- 如果 Link 字段取值为 DIS，则表示该 IRF 端口还没有和任何 IRF 物理端口绑定。请根据组网需要在 IRF 端口视图下使用 **port group interface** 命令进行绑定。
- 如果 Link 字段取值为 DOWN，请使用 **display irf link** 命令进一步检查 IRF 物理端口的状态是否为 UP。
  - 如果 IRF 物理端口的状态为 UP，但 IRF 端口的状态为 DOWN，原因可能是 IRF 端口的配置未激活。请在系统视图下执行 **irf-port-configuration active** 命令激活 IRF 端口。
  - 如果 IRF 物理端口的状态不是 UP，请参照步骤(5)定位 IRF 物理端口的问题。
- 如果 Link 字段取值为 TIMEOUT，表明 IRF Hello 报文超时，IRF 链路通信存在问题。可参照以下步骤先定位 IRF 报文超时问题。
  - 确认是否因为对端 IRF 端口状态异常，导致 IRF 报文无法互通：登录 IRF 链路的对端设备，在对端设备上执行 **display irf topology** 和 **display irf link**，根据显示的状态信息进行定位。
  - 确认是否存在网络环路，导致 IRF 报文丢包：使用 **display counters rate inbound interface** 命令查看 IRF 物理端口的报文速率统计信息，确认 IRF 链路上是否存在报文风暴。如果存在报文风暴，请检查是否存在物理环路以及 VLAN 和 STP 配置是否正确等，先解决报文风暴问题。
  - 使用 **display device** 命令检查网板状态是否正常。如果不正常，请先定位网板问题。
- 如果 Link 字段取值为 ISOLATE，表明该成员设备处于隔离状态。执行 **display logbuffer | include** “STM stackability check”，并根据显示结果处理：
  - 如果显示信息中包含“STM stackability check: Product series is inconsistency”字样，则说明成员设备的型号不符合 IRF 要求，请参考步骤(7)处理。
  - 如果显示信息中包含“STM stackability check: Product xxx is inconsistency”字样，xxx 取值可能为 system working mode 等，则说明当前系统参数配置不符合 IRF 要求，请参考步骤(8)处理。

(5) 检查 IRF 物理端口的状态，使其变成 UP 状态。

请通过 **display irf link** 命令查看 IRF 物理端口的状态。如果显示信息中：

- Interface 字段取值为 disable，表示该 IRF 端口还没有和 IRF 物理端口绑定。
- Interface 字段为物理接口的名称，请继续检查 Status 字段。Status 字段的取值及含义如下：
  - UP：链路 up，无需处理
  - DOWN：链路 down，请检查 IRF 物理端口的光模块/光纤或者电缆是否工作正常。请使用符合产品要求的物理接口作为 IRF 物理端口，使用符合产品要求的线缆来连接 IRF 物理端口，并执行步骤(6)。
  - ADM：表示该接口通过 **shutdown** 命令被关闭，即管理状态为关闭。您需要执行 **undo shutdown** 命令将其开启。
  - ABSENT：接口不存在。请插入单板或接口模块扩展卡。

(6) 检查 IRF 物理连线是否符合要求。

可通过以下步骤来定位 IRF 物理连接问题：

a. 在每台成员设备上通过 **display irf configuration** 命令查看 IRF 端口与 IRF 物理端口的绑定关系。检查绑定的物理接口和实际连接的物理接口是否一致，如果不一致，请重新配置绑定关系或重新进行物理连接。

b. 检查 IRF 物理端口的连接状况，是否满足相邻设备的连接要求。连接两台相邻的成员设备时，一台设备上 IRF-Port1 绑定的 IRF 物理端口只能和邻居成员设备 IRF-Port2 绑定的 IRF 物理端口相连。且当两台成员设备组建 IRF 时，只能使用链型拓扑，不允许使用环形拓扑。

(7) 检查成员设备的硬件是否符合 IRF 的要求。

当设备的品牌和款型均相同时，支持组建 IRF。

设备工作在 IRF 模式时，不支持如下类型接口模块：

语音模块

WLAN 模块

POS 终端接入接口模块

数字调制解调器接口模块

模拟 Modem 模块

对于如下类型的接口模块，必须满足以下条件，才支持工作在 IRF 模式：

网络数据加密模块：主从设备必须同时安装。

以太网交换模块：主从设备的以太网交换模块支持的 VLAN 数量必须相同。

(8) 检查系统参数配置是否满足 IRF 的要求。

部分产品会要求设备的 VXLAN 硬件资源工作模式、路由硬件资源工作模式、以及等价路由条数等系统参数的配置相同，否则无法组建 IRF。（不同产品的具体要求不同，请以设备的实际情况为准）

- 使用 **display hardware-resource** 命令可查看设备的硬件资源工作模式，使用 **hardware-resource vxlan**、**hardware-resource routing-mode** 命令可将设备的硬件资源工作模式修改为相同值。修改硬件资源工作模式后请重启该设备，使修改的工作模式生效。
- 使用 **display max-ecmp-num**、**display ipv6 max-ecmp-num** 命令可查看系统支持的最大等价路由条数，使用 **max-ecmp-num**、**ipv6 max-ecmp-num** 命令可将系统支持的最大等价路由条数修改为相同值。修改系统支持的最大等价路由条数后请重启该设备，使修改的配置生效。

(9) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：HH3C-STACK-MIB

- hh3cStackPhysicalIntfLinkDown(1.3.6.1.4.1.25506.2.91.6.0.8)
- hh3cStackPhysicalIntfRxTimeout (1.3.6.1.4.1.25506.2.91.6.0.9)

相关日志

- STM/3/STM_LINK_DOWN
- STM/2/STM_LINK_TIMEOUT
- STM/6/STM_LINK_UP
- STM/4/STM_SAMEMAC
- STM/3/STM_SOMER_CHECK

6.1.2 IRF 成员设备异常重启

1. 故障描述

堆叠过程中发生了主设备或者备设备异常重启，导致堆叠分裂。

2. 常见原因

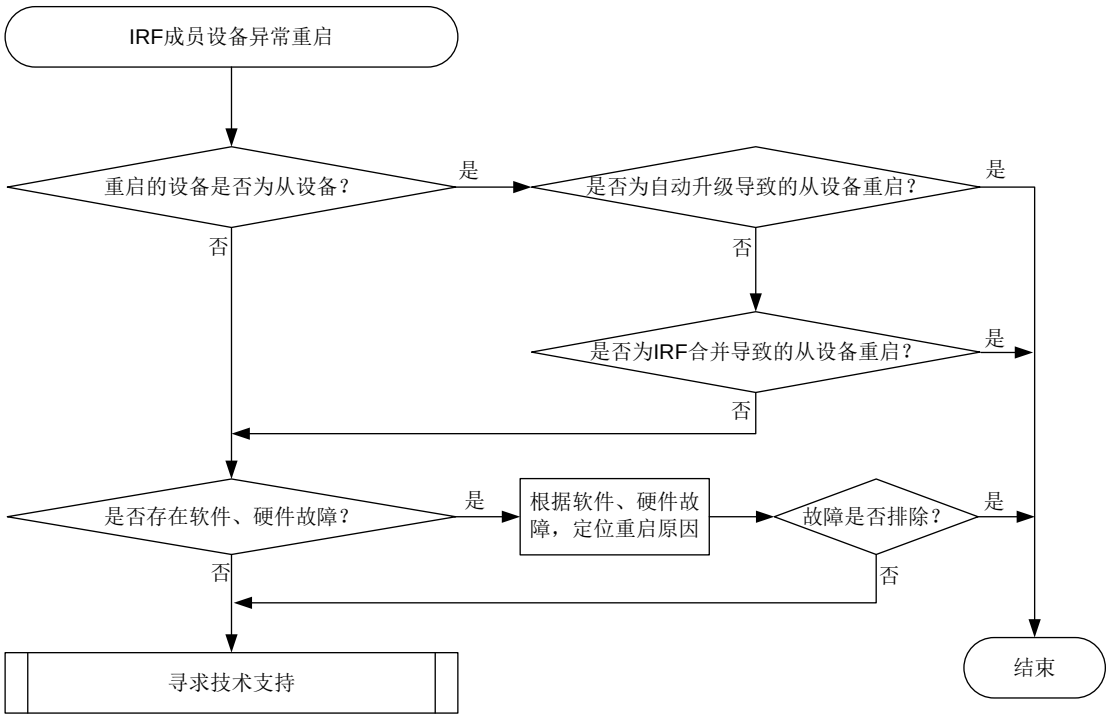
本类故障的常见原因主要包括：

- 从设备自动重启来完成软件版本的升级。
- IRF 合并，导致从设备重启。
- 设备软件或者硬件故障，导致设备异常重启，来尝试修复故障。

3. 故障分析

本类故障的诊断流程如图 33 所示。

图33 IRF 成员设备异常重启故障诊断流程图



4. 处理步骤

(1) 检查重启的设备是否为从设备。

- 如果是从设备，请执行步骤(2)。
- 如果不是从设备，是主设备，请执行步骤(4)。

(2) 检查从设备是否因为自动加载启动文件，升级导致的重启。

- 如果从设备是因为自动加载启动文件，升级导致的重启，则该重启为正常重启，无需处理。
- 如果从设备不是因为自动加载启动文件，升级导致的重启，请继续执行步骤(3)。

您可通过以下方式确认从设备的重启原因：IRF 要求所有成员设备上运行的软件版本必须一致。当 IRF 开启了启动文件的自动加载功能，且有新设备加入 IRF 时，如果新设备的软件版本和主设备的软件版本不一致，则新设备会自动从主设备下载启动文件，然后使用新的启动文件重启并以从设备角色加入 IRF。在 Probe 视图下，执行 **`display system internal irf msg`** 命令，如果显示信息中有“`Version is different, and the sender CPU MAC is xxxx-xxxx-xxxx (chassis xx slot xx).`”类似信息，表示 CPU MAC 为 *xxxx-xxxx-xxxx* 的从设备是因为自动加载启动文件，升级导致的重启。

(3) 检查是否因为 IRF 合并导致的从设备重启。

- 如果从设备重启原因为 IRF 合并，请追查 IRF 分裂、合并的原因，并排除安全隐患，以免再次因为同样的原因导致 IRF 分裂、合并。
- 如果从设备重启原因不是 IRF 合并，请继续执行步骤(4)。

您可通过以下方式确认从设备的重启原因是否为 IRF 合并：

- 设备重启后，在 IRF 中执行 **display kernel reboot** 命令查看设备的重启原因。如果 Reason 字段取值为 0x7，则表示从设备重启原因为 IRF 合并，Slot 表示触发重启事件的 Slot 的编号，Target Slot 表示实际发生重启的 Slot 的编号。

```
<Sysname> display kernel reboot 1
-------------------- Reboot record 1 --------------------
Recorded at           : 2021-12-06  00:10:05.440616
Occurred at           : 2021-12-06  00:10:05.440616
Reason                : 0x7
Thread                : STM_Main (TID: 232)
Context               : thread context
Slot                  : 1
Target Slot           : 2
Cpu                   : 0
VCPU ID               : 2
Kernel module info    : module name (system) module address (0xffffffffc0074000)
                        module name (addon) module address (0xffffffffc0008000)
```

- 在 IRF 的 Probe 视图下执行 **display system internal irf msg | include reboot** 命令，如果可以看到主设备发送了重启报文，则表示从设备重启原因为 IRF 合并。

```
19> Send reboot pkt, src_addr 5e40-08d9-0104 (chassis 1 slot 1), at 2022/1/5
15:42:48:386
```

(4) 检查是否有软件和硬件故障导致成员设备异常重启。

通过 **display version** 命令，可以查看成员设备/单板上次重启的原因，根据重启原因，以及表 2 所示的建议操作进行处理。

```
<Sysname> display version
…
Reboot Cause   :     ColdReboot
[SubSlot 0] 24GE+4SFP Plus+POE
```

表2 设备重启原因以及建议操作

Reboot Cause 字段的取值	重启原因说明	建议操作
AutoUpdateReboot	自动更新版本后重启	正常，无需处理
BootwareBackupReboot	Bootware 备份区重启	请收集日志、诊断日志，联系技术支持人员处理
ColdReboot	设备掉电	检查设备的供电环境，确保供电正常
CryptographicModuleSelftestsFailedReboot	算法库自检失败	请及时升级软件版本
CryptotestFailReboot	加密算法库自检失败	请及时升级软件版本
DeadLoopReboot	软件检测到死循环	请收集日志、诊断日志和重启slot的**display kernel deadloop 20 verbose**的显示信息，联系技术支持人员处理
GoldMonReboot	GOLD（Generic OnLine Diagnostics，通用在线诊断）检测到异常	可通过以下操作确认重启原因： • **display diagnostic content** 命令，通过 Correct-action 字段可看到 GOLD 检测到异常时的纠错动作是重启，测试发生的时间以及测试

Reboot Cause 字段的取值	重启原因说明	建议操作
		发现的问题 • **display diagnostic event-log** 命令查看测试的详细执行信息 根据以上显示信息找到具体的重启原因，并进行定位
IRFMergeReboot	IRF合并	IRF链路故障会导致IRF分裂，IRF链路恢复后，IRF会自动合并。请追查故障的IRF链路，并排除安全隐患，以免再次因为同样的原因导致IRF分裂、合并
KernelAbnormalReboot	CPU、主机内存或软件问题导致系统内核错误	请收集日志、诊断日志和诊断命令**display kernel exception 10 verbose**、**display kernel reboot 20 verbose**的信息，联系技术支持人员处理
KeyReboot	触碰了<RESET>键	避免误操作
LicenseTimeoutReboot	License 过期	请及时安装正式版本的License
MemoryexhaustReboot	内存消耗，低于门限值	ACL表项太多等原因会导致内存占用率高，确认内存占用率高的原因，解决内存占用率高故障
PdtReboot	产品驱动要求的重启	请收集日志、诊断日志，联系技术支持人员处理
UserReboot	通过命令行、网管或 Web 页面等方式主动重启设备	正常，无需处理
WarmReboot	原因可能有多种，例如单板虚插针脚接触不良导致单板重启等	请收集日志、诊断日志，联系技术支持人员处理
WatchDogReboot	CPU、内存、软件或其它硬件故障，导致看门狗监测到系统异常，重启设备	根据**display hardware-failure-detection**命令显示的故障修复信息定位故障原因，消除安全隐患

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 假设 slot 16 为主用主控板，以备用主控板 slot 17 重启为例，请收集以下命令的显示信息。
  - 请在任意视图下执行以下命令：

```
display version
display device
display diagnostic-information
display kernel deadloop 20 verbose slot 16
display kernel exception 10 verbose slot 16
display kernel reboot 20 verbose slot 16
```

- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- DEV/1/AUTO_SWITCH_FAULT_REBOOT
- DEV/5/BOARD_REBOOT
- DEV/1/BOARD_RUNNING_FAULT_REBOOT
- DEV/5/CHASSIS_REBOOT
- DEV/5/SUBCARD_REBOOT
- DEV/5/SYSTEM_REBOOT
- STM/4/STM_MERGE

7 二层技术-以太网交换类故障处理

7.1 生成树故障处理

7.1.1 设备连接成环时业务中断

1. 故障描述

多台设备通过物理链路连接成环时，业务流量中断。

2. 常见原因

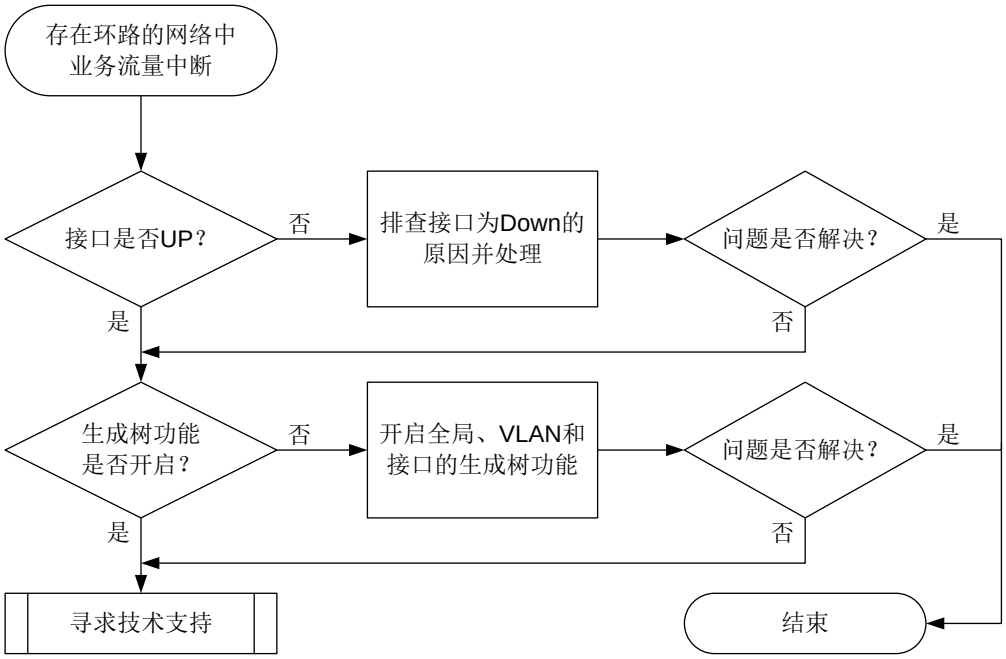
本类故障的常见原因包括：

- 设备接口的物理状态为 DOWN。
- 设备的生成树功能处于关闭状态。

3. 故障分析

本类故障的诊断流程如图 34 所示。

图34 设备连接成环时业务中断的故障诊断流程图



4. 处理步骤

(1) 检查承载业务流量的接口状态是否为 UP。

a. 检查接口的物理状态是否为 UP。

执行 **display interface brief** 命令，通过“Link”字段查看网络中的接口物理状态是否为 UP，例如：

```
<Sysname> 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
InLoop0                           UP   UP(s)    --
MGE0/0/0                          DOWN DOWN     --
NULL0                             UP   UP(s)    --
REG0                              UP   --       --

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface                         Link Speed   Duplex Type PVID Description
GE1/0/1                           ADM  auto    A      A    1
GE1/0/2                           UP   auto    A      A    1
GE1/0/3                           DOWN auto    A      A    1
```

– 如果网络中接口的状态为 UP，请执行步骤 b。

- 如果网络中接口的状态为 ADM，请在接口视图下执行 **undo shutdown** 命令开启该接口。如果接口的状态仍为 DOWN，请进行接口链路以及相关配置的排查；如果此时接口的状态为 UP，但是故障仍未解决，请执行步骤 b。
- 如果网络中接口的状态为 DOWN，请进行接口链路以及相关配置的排查。接口状态恢复 UP 后，如果故障仍未解决，请执行步骤 b。

b. 检查接口的数据链路层协议状态是否为 UP。接口的数据链路层协议为 DOWN 的接口无法参与生成树拓扑的计算。

执行 **display interface** 命令，通过“Line protocol state”字段查看网络中的接口数据链路层协议状态是否为 UP，例如：

```
<Sysname> display interface gigabitethernet 1/0/2
GigabitEthernet1/0/2
Current state: UP
Line protocol state: DOWN(LAGG)
...
```

DOWN(*protocols*)表示接口的数据链路层被一个或者多个协议模块关闭。*protocols* 为多个协议的任意组合，可能的协议如下：

- DLDP：由于 DLDP 模块检测到单通而关闭接口的数据链路层。
- LAGG：聚合接口中没有选中的成员端口而关闭接口的数据链路层。
- BFD：由于 BFD 模块检测到链路故障而关闭接口的数据链路层。
- VBP：由于配置二层转发功能后而关闭接口的数据链路层。

如果接口的数据链路层被上述协议关闭，请检查并修改这些模块的配置，使得接口的数据链路层协议状态恢复为UP。如果接口的数据链路层协议状态恢复为UP后，故障仍未解决，请执行步骤（2）。

(2) 检查设备的生成树功能是否开启。

a. 检查设备上全局生成树功能是否开启。

执行 **display stp** 命令：

- 如果出现如下显示信息，则表示全局的生成树协议未开启：

```
<Sysname> display stp
 Protocol status    : Disabled
 Protocol Std.      : IEEE 802.1s
 Version            : 3
 Bridge-Prio.       : 32768
 MAC address        : 2eae-3769-0200
 Max age(s)         : 20
 Forward delay(s)   : 15
 Hello time(s)      : 2
 Max hops           : 20
 TC Snooping        : Disabled
```

```
<Sysname> display stp
STP is not configured.
```

请在系统视图下执行 **stp global enable** 命令开启全局的生成树功能。

– 如果出现生成树的状态和统计信息（如下所示），则说明全局的生成树功能已经开启，请继续执行步骤 b。

```
<Sysname> display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID           : 32768.2eae-3769-0200
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 32768.2eae-3769-0200, 0
 RegRoot ID/IRPC     : 32768.2eae-3769-0200, 0
 RootPort ID         : 0.0
 BPDU-Protection     : Disabled
 Bridge Config-
 Digest-Snooping     : Disabled
 TC or TCN received  : 0
 Time since last TC  : 0 days 2h:49m:11s

----[Port54(GigabitEthernet1/0/2)][DOWN]----
 Port protocol       : Enabled
 Port role           : Disabled Port
 Port ID             : 128.54
 Port cost(Legacy)   : Config=auto, Active=200000
 Desg.bridge/port    : 32768.2eae-3769-0200, 128.54
 Port edged          : Config=disabled, Active=disabled
 Point-to-Point      : Config=auto, Active=false
 Transmit limit      : 10 packets/hello-time
 TC-Restriction      : Disabled
 Role-Restriction    : Disabled
 Protection type     : Config=none, Active=none
 MST BPDU format     : Config=auto, Active=802.1s
 Port Config-
 Digest-Snooping     : Disabled
 Rapid transition    : False
 Num of VLANs mapped : 1
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
 BPDU sent           : 0
          TCN: 0, Config: 0, RST: 0, MST: 0
 BPDU received       : 0
          TCN: 0, Config: 0, RST: 0, MST: 0
```

b. （仅生成树模式为 PVST 时适用，非 PVST 模式请继续执行步骤 c）检查 VLAN 的生成树功能是否开启。

在系统视图下，执行 **display this** 命令，查看是否存在 **undo stp vlan enable** 命令的配置，例如：

```
[Sysname] display this
...
#
 undo stp vlan 2 enable
 stp mode pvst
 stp global enable
```

```
#
...
```

如果存在上述配置且网络中需要开启对应 VLAN 的生成树功能，请在系统视图下执行 **stp vlan enable** 命令，开启 VLAN 的生成树功能。

c. 检查接口的生成树功能是否开启。

执行 **display stp** 命令，查看是否存在生成树功能未开启的接口，例如：

```
<Sysname> display stp
...
----[Port2(GigabitEthernet1/0/1)][DISABLED]----
 Port protocol       : Disabled
...
```

请在需要参与生成树计算的接口视图下执行 **stp enable** 命令，开启接口的生成树功能。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

7.1.2 接入生成树网络的用户终端设备发生掉线

1. 故障描述

用户终端设备接入生成树网络时，连接终端设备的接口发生闪断，业务长时间丢包，造成终端设备掉线。

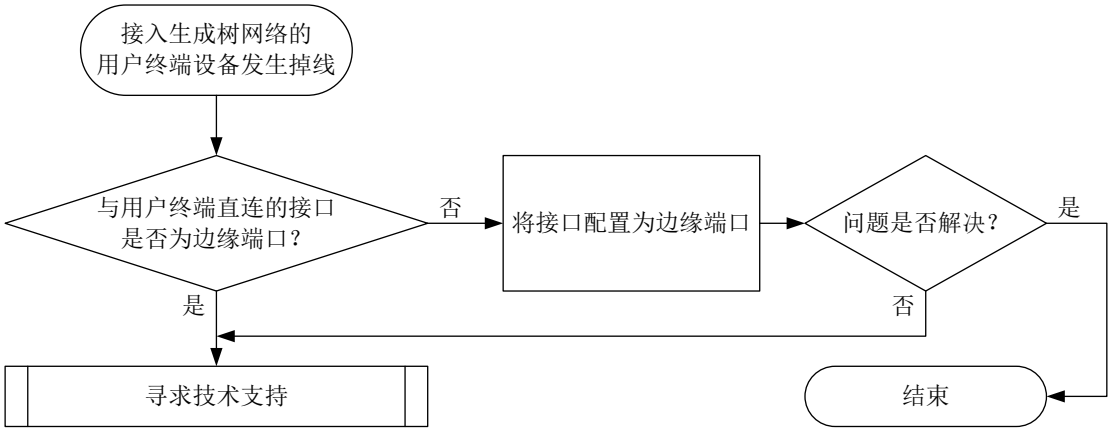
2. 常见原因

本类故障的常见原因为：连接用户终端设备的接口未被配置为边缘端口。

3. 故障分析

本类故障的诊断流程如图 35所示。

图35 接入生成树网络的用户终端设备发生掉线的故障诊断流程图



4. 处理步骤

(1) 检查生成树网络中与用户终端设备直连的接口是否为边缘端口。

在与用户终端设备直连的生成树网络设备上执行 **display stp** 命令，查看与用户终端设备直连的接口是否为边缘端口，例如：

```
<Sysname> display stp
...
----[Port2(GigabitEthernet1/0/1)][FORWARDING]----
 Port protocol       : Enabled
 Port role           : Designated Port
 Port ID             : 128.2
 Port cost(Legacy)   : Config=auto, Active=20
 Desg.bridge/port    : 32768.2eae-3769-0200, 128.2
 Port edged          : Config=enabled, Active=enabled
 Point-to-Point      : Config=auto, Active=true
 Transmit limit      : 10 packets/hello-time
 Protection type     : Config=none, Active=none
 Rapid transition    : True
 Port times          : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s
...
```

- 如果与用户终端设备直连的接口是边缘端口，请执行步骤（2）。
- 如果与用户终端设备直连的接口不是边缘端口，请进入该接口视图，并执行 **stp edged-port** 命令，将该端口配置为边缘端口。

说明

在接口下不能同时配置边缘端口和环路保护功能，执行 **stp edged-port** 命令时，如果设备打印如下错误提示信息，说明当前接口已经配置了环路保护功能。此时需要先执行 **undo stp loop-protection** 命令关闭环路保护功能，才能将该端口配置为边缘端口。

```
Failed to enable edged-port on GigabitEthernet1/0/1, because loop-protection is
enabled.
```

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

- STP/6/STP_DETECTED_TC

7.1.3 非 0 实例端口状态为主端口且无法调整

1. 故障描述

在 MSTP 网络中，设备上除了 MSTI 0 之外的其他实例，本不应该是主端口角色的端口被计算为了主端口，且端口角色无法通过调整优先级、开销值等参数来改变。

2. 常见原因

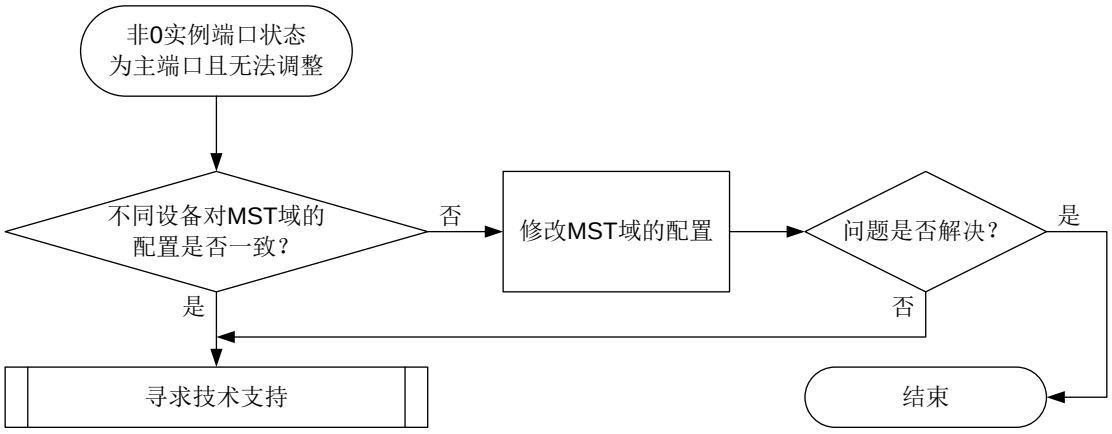
本类故障的常见原因为：同一 MST 域内，不同设备对 MST 域的配置不一致。

3. 故障分析

如果两台设备对 MST 域的配置不一致，则设备会认为对端设备与本端设备不在同一个 MST 域中，导致与域内设备相连的端口也被计算为了主端口。所以本类故障的诊断思路为：检查同一 MST 域内设备的 MST 域配置信息，确保各个设备的配置保持一致。

本类故障的诊断流程如 7.1.2 3. 图 35 所示。

图36 非 0 实例端口状态为主端口且无法调整的故障处理流程图



4. 处理步骤

(1) 检查同一 MST 域内的设备对于 MST 域的域名、修订级别以及 VLAN 映射表配置是否相同，并确保这些参数的配置一致。

执行 **display stp region-configuration** 命令，显示设备生效的 MST 域配置信息。例如：

```
<Sysname> display stp region-configuration
```

```
Oper Configuration
  Format selector      : 0
  Region name          : hello
  Revision level       : 0
  Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

  Instance   VLANs Mapped
  0          21 to 4094
  1          1 to 10
  2          11 to 20
```

- Region name：MST 域的域名，在系统视图下执行 **stp region-configuration** 命令进入 MST 域视图后，通过 **region-name** 命令进行配置。
- Revision level：MST 域的修订级别，在系统视图下执行 **stp region-configuration** 命令进入 MST 域视图后，通过 **revision-level** 命令进行配置。
- Instance VLANs Mapped：MST 域的 VLAN 映射关系，在系统视图下执行 **stp region-configuration** 命令进入 MST 域视图后，可以通过 **instance** 命令或 **vlan-mapping modulo** 命令进行配置。

如果同一 MST 域内不同设备的上述参数配置不相同，请执行上述操作将参数的配置修改为一致配置完 MST 域的相关参数后，必须在 MST 域视图下执行 **active region-configuration** 命令，用户对 MST 域的配置才能激活并生效，否则 MST 域仍会按照之前的配置生效。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无。

相关日志

无。

7.2 以太网链路聚合故障处理

7.2.1 聚合接口无法 UP

1. 故障描述

当两台设备间通过链路聚合连接时，通过 **display interface** 命令查看聚合接口处于 down 状态。

2. 常见原因

本类故障的常见原因主要包括：

- 聚合接口配置错误。
- 成员端口物理链路故障。
- LACP 协议报文收发故障。

3. 故障分析

本类故障的诊断思路如下：

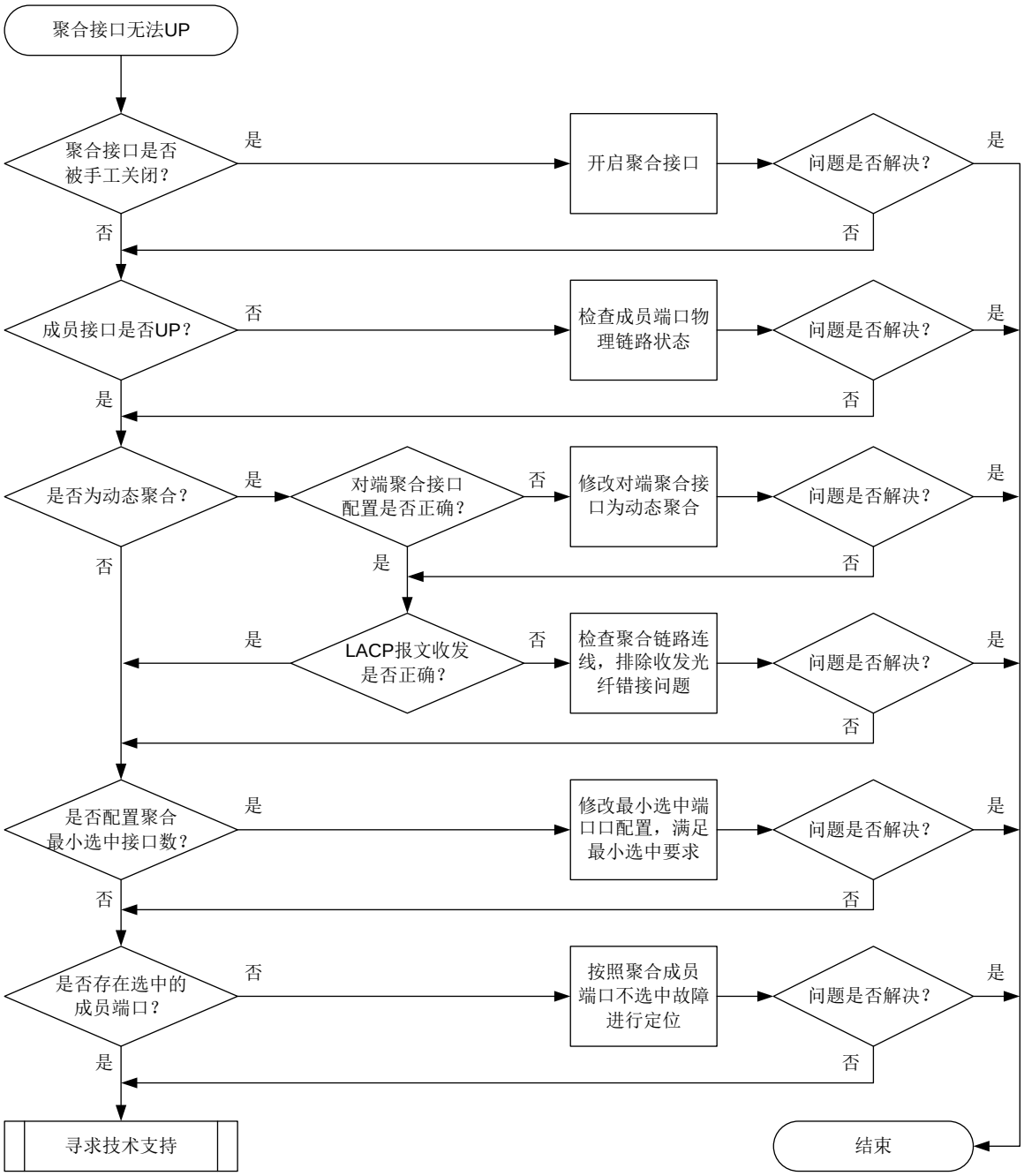
(1) 通过 **display link-aggregation verbose** 查看成员端口是否处于选中状态，如果处于非选中状态，则通过 **display interface** 命令查询成员端口物理状态是否 UP，排除端口物理故障影响。

(2) 检查本端和对端聚合接口配置，排除配置问题。

(3) 使用 **debugging link-aggregation lacp packet** 命令查看动态聚合的成员端口 LACP 协议交互情况。

本类故障的诊断流程如图 37 所示。

图37 聚合接口无法 UP 的故障诊断流程图



4. 处理步骤

(1) 排查物理连线是否准确。

根据聚合接口的组网规划进行线路检查，确认物理链接线路是否完全按照规划连接。

如果物理连线正确，则执行步骤(2)。

(2) 聚合接口是否被手工关闭。

执行 **display interface** 命令查看聚合接口的物理状态，如果显示为“Administratively DOWN”，则表示聚合接口被手工关闭，请执行 **undo shutdown** 命令开启聚合接口。如果聚合接口未被手工关闭，则执行步骤(3)。

(3) 聚合组中成员端口是否 UP。

执行 **display interface** 命令查看聚合组中的成员端口是否处于 UP 状态，如果没有 UP，请按照端口不 UP 故障流程处理。

如果端口处于 UP 状态，则执行步骤(4)。

以如下显示为例，三层聚合组 1 中成员端口 GigabitEthernet1/0/1 处于非选中状态。执行 **display interface** 命令查看 GigabitEthernet1/0/1 的物理状态时，物理状态显示为“DOWN”，使成员端口 GigabitEthernet1/0/1 处于非选中状态。

```
<Sysname> display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1          U       32768    1
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
IPv6 packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
loopback: not set, promiscuous mode: not set
1000Mb/s, Full-duplex, link type: autonegotiation,
flow-control: disabled
Output queue - Urgent queuing: Size/Length/Discards 0/1024/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 5 days 3 hours 6 minutes
Last clearing of counters: 09:59:36 Wed 12/26/2021
Current system time:2018-12-26 10:33:19
Last time when physical state changed to up:2021-12-21 07:27:13
Last time when physical state changed to down:2021-12-21 07:27:10
 Last 200 second input: 6 packets/sec 1728 bytes/sec 0%
```

```
Last 200 second output: 0 packets/sec 22 bytes/sec 0%
Input (total):  10694 packets, 2944465 bytes
         951 unicasts, 3337 broadcasts, 6406 multicasts, 0 pauses
Input (normal):  10694 packets, 2944465 bytes
         951 unicasts, 3337 broadcasts, 6406 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, 0 parity errors
Output (total): 1325 packets, 83462 bytes
         1321 unicasts, 4 broadcasts, 0 multicasts, 0 pauses
Output (normal): 1325 packets, 83462 bytes
         1321 unicasts, 4 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, 0 no carrier
```

(4) 判断聚合接口是否为动态聚合。

- 如果聚合接口为动态聚合，则检查对端聚合接口的配置是否正确，即对端聚合接口是否为动态聚合。在任意视图下执行 **display link-aggregation verbose** 命令，查看链路两端聚合接口的聚合模式，确保两端聚合模式相同。

  以三层聚合接口为例，显示“Aggregation Mode: Dynamic”时，表示该聚合接口为动态聚合：

```
<Sysname> display link-aggregation verbose route-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    61       2                      {ACDEF}
  GE1/0/2             S        32768    62       2                      {ACDEF}
  GE1/0/3             S        32768    63       2                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/2             32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/3             32768    113      2        0x8000, 000f-e267-57ad {ACDEF}
```

  如果配置不正确，则修改对端聚合接口为动态聚合；如果配置正确，则执行 **debugging link-aggregation lacp packet** 命令确认 LACP 报文收发是否正确。

执行 **debugging link-aggregation lacp packet** 命令后，查看成员端口 send 信息中 Actor 信息和 receive 信息中 Partner 信息。如果 sys-mac、key 和 port-index 字段的显示不一致，则 LACP 协议报文收发不正常，请排除收发光纤错接问题；如果 sys-mac、key 和 port-index 字段的显示一致，则 LACP 协议报文收发正常，请执行步骤(5)。

打开聚合组成员端口 GigabitEthernet1/0/1 的 LACP 报文调试信息开关，查看该端口收发 LACP 协议报文的情况。

```
<Sysname> debugging link-aggregation lacp packet all interface gigabitethernet 1/0/1
*Nov  2 15:51:21:15 2007 Sysname LAGG/7/Packet: PACKET.GigabitEthernet1/0/1.send.
 size=110, subtype =1, version=1
 Actor: type=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=0x1, pri=0x8000,
port-index=0x2, state=0xc5
 Partner: type=2, len=20, sys-pri=0x0, sys-mac=0000-0000-0000, key=0x0, pri=0x0,
port-index=0x0, state=0x32
 Collector: type=3, len=16, col-max-delay=0x0
 Terminator: type=0, len=0
*Nov 2 15:55:21:15 2007 Sysname LAGG/7/Packet: PACKET.GigabitEthernet1/0/1.receive.
size=110, subtype =1, version=1
 Actor: type=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc00-0000, key=0x1, pri=0x8000,
port-index=0x6, state=0xd
 Partner: type=2, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=0x1,
pri=0x8000, port-index=0x2, state=0xc5
 Collector: type=3, len=16, col-max-delay=0x0
 Terminator: type=0, len=0
```

- 如果聚合接口为静态聚合，则执行步骤(5)。

(5) 查看聚合接口下最小选中端口的配置是否影响成员端口选中。

在聚合接口视图下执行 **display this** 命令，如果存在 **link-aggregation selected-port minimum** 的配置，请修改最小选中端口数值，使其满足最小选中要求。当聚合组内能够被选中的成员端口数增加至不小于配置值时，这些成员端口都将变为选中状态，对应聚合接口的链路状态也将变为 UP。

如果聚合接口下最小选中端口的配置未影响成员端口选中，则执行步骤(6)。

以如下显示为例，三层聚合接口 1 下配置的最小选中端口数为 2，而三层聚合接口 1 对应的聚合组的成员端口仅有一个，所以该成员端口处于非选中状态。

```
[Sysname-Route-Aggregation1] display this
#
interface Route-Aggregation1
 link-aggregation selected-port minimum 2
#
return
[Sysname-Route-Aggregation1] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
```

```
Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1          U       32768    1
```

(6) 聚合组内是否存在选中的成员端口。

如果聚合组内不存在选中的成员端口，则请参见“7.2.3 聚合成员端口无法选中”故障进行定位；如果聚合组内存在选中的成员端口，则执行步骤(7)。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

7.2.2 聚合接口流量负载分担不均

1. 故障描述

当两台设备通过链路聚合连接时，通过 **display counters rate** 命令查看聚合成员端口出方向流量速率，某些成员端口速率特别小或者根本没有。

2. 常见原因

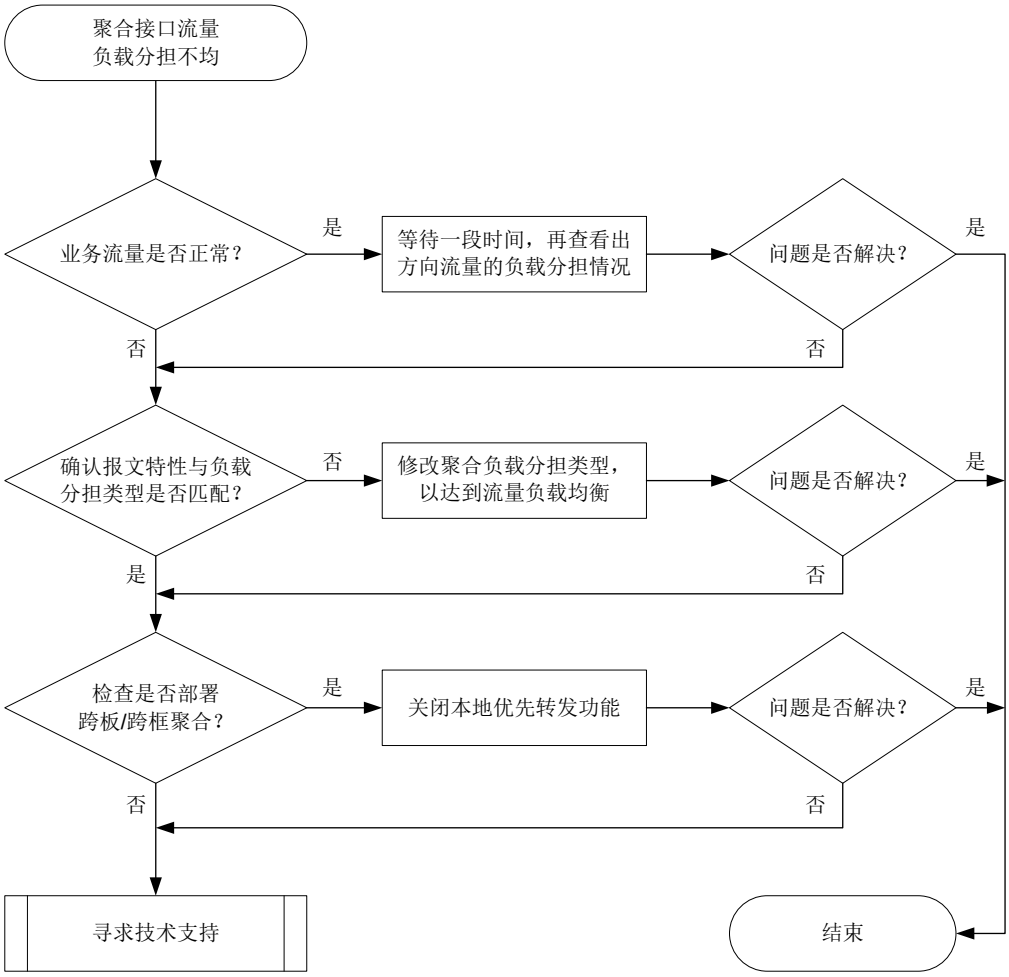
本类故障的常见原因主要为聚合负载分担方式配置错误。

3. 故障分析

本类故障的诊断思路为确认聚合接口转发的报文的特征，并查看聚合负载分担类型是否和报文特性匹配。

本类故障的诊断流程如图 38 所示。

图38 聚合接口流量负载分担不均的故障诊断流程图



4. 处理步骤

(1) 用户业务流量是否正常。

如果用户业务流量正常，则等待一段时间，再执行 **display counters rate** 命令查看聚合成员端口出方向流量速率，确认聚合成员端口流量是否恢复负载分担：

- 如果已恢复负载分担，则无需处理。
- 如果未恢复负载分担，则执行步骤(2)。

如果用户业务流量不正常，则执行步骤(2)。

(2) 查看聚合负载分担类型与报文特征是否匹配。

通过执行 **display link-aggregation load-sharing mode** 命令查看聚合负载分担类型，如果与报文特征不匹配，则通过以下命令调整聚合负载分担类型：

- 在系统视图下执行 **link-aggregation global load-sharing mode** 命令调整全局的负载分担类型。
- 在聚合接口视图下执行 **link-aggregation load-sharing mode** 命令调整聚合接口的负载分担类型。

针对不同业务流量，不同产品调整的负载分担类型不同，请参见命令参考手册。

如果聚合负载分担类型与报文特征匹配，则执行步骤(3)。

(3) 检查是否部署跨板/跨框聚合。

在 IRF 环境下，如果部署跨板/跨框聚合，则在系统视图下使用 **undo link-aggregation load-sharing mode local-first** 命令关闭本地优先转发功能。如果关闭本地优先转发功能，则可能导致跨板/跨框流量过大，影响 IRF 系统稳定，请根据实际情况进行操作。

如果未部署跨板/跨框聚合，则执行步骤(4)。

需要注意，跨板/跨框流量不能过大，否则可能影响 IRF 系统稳定。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

7.2.3 聚合成员端口无法选中

1. 故障描述

当两台设备通过链路聚合连接时，发现聚合组成员端口处于非选中状态，聚合失败。

2. 常见原因

本类故障的常见原因主要包括：

- 链路连通性故障。
- 本端和对端的操作 key、属性类配置不一致。
- 聚合成员端口数配置错误。

3. 故障分析

本类故障的诊断思路如下：

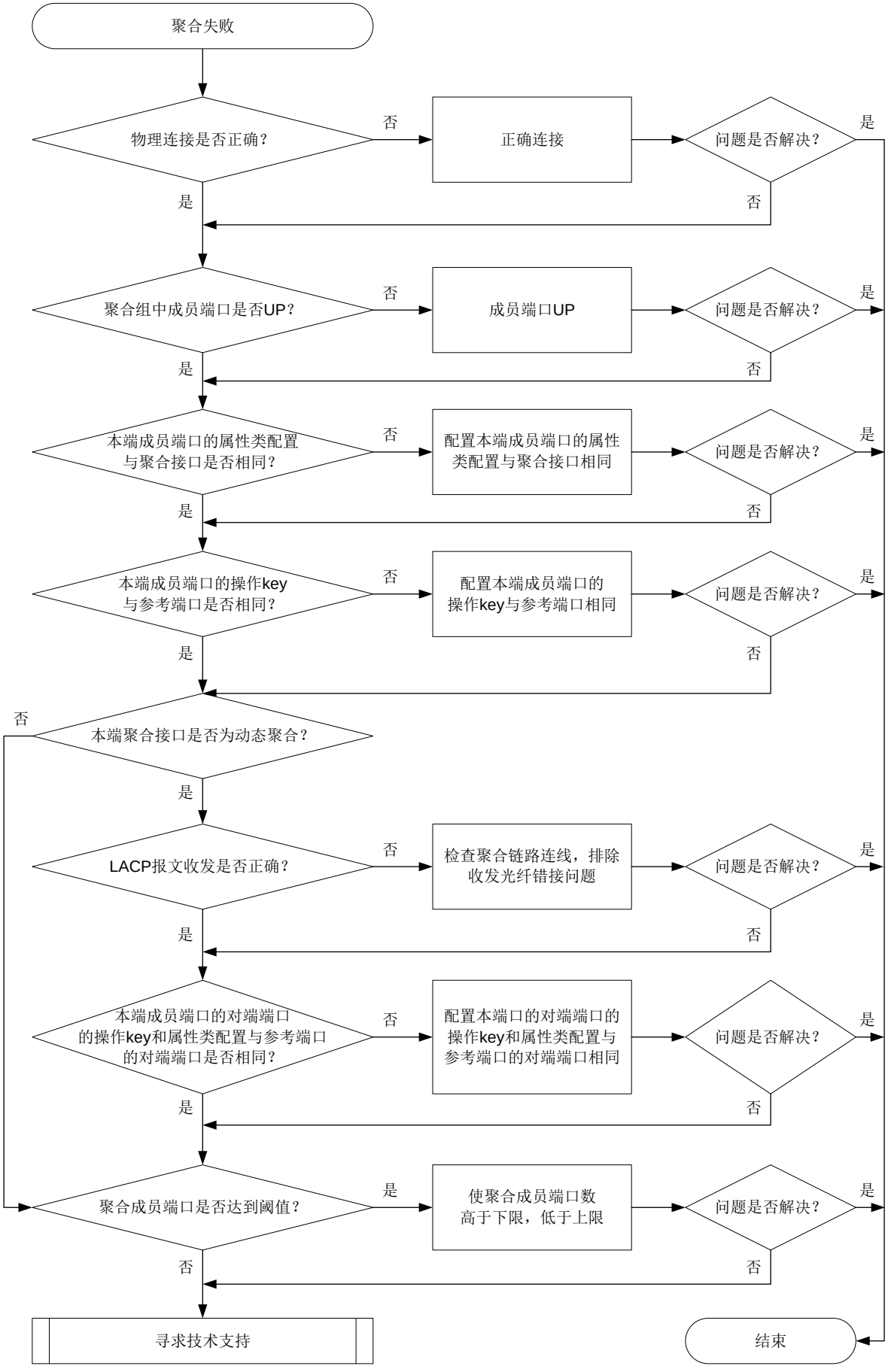
(1) 查看成员端口是否 UP，排除端口物理故障影响。

(2) 使用 **debugging link-aggregation lacp packet** 命令查看动态聚合的成员端口 LACP 协议交互情况。

(3) 检查本端和对端聚合接口配置，排除配置影响。

本类故障的诊断流程如图 39 所示。

图39 聚合成员端口无法选中的故障诊断流程图


聚合失败
物理连接是否正确？
否
正确连接
问题是否解决？
是
否
是
聚合组中成员端口是否UP？
否
成员端口UP
问题是否解决？
是
否
是
本端成员端口的属性类配置与聚合接口是否相同？
否
配置本端成员端口的属性类配置与聚合接口相同
问题是否解决？
是
否
是
本端成员端口的操作key与参考端口是否相同？
否
配置本端成员端口的操作key与参考端口相同
问题是否解决？
是
否
是
否
本端聚合接口是否为动态聚合？
是
LACP报文收发是否正确？
否
检查聚合链路连线，排除收发光纤错接问题
问题是否解决？
是
否
是
本端成员端口的对端端口的操作key和属性类配置与参考端口的对端端口是否相同？
否
配置本端口的对端端口的操作key和属性类配置与参考端口的对端端口相同
问题是否解决？
是
否
是
聚合成员端口是否达到阈值？
是
使聚合成员端口数高于下限，低于上限
问题是否解决？
是
否
否
寻求技术支持
结束

4. 处理步骤

(1) 排查物理连线是否正确。

根据聚合接口的组网规划进行线路检查，确认物理链接线路是否完全按照规划连接。

如果物理连线正确，则执行步骤(2)。

(2) 聚合组中成员端口是否 UP。

通过 **display interface** 命令查看聚合组中的成员端口是否处于 UP 状态，如果没有 UP，请按照端口不 UP 故障流程处理。

如果端口处于 UP 状态，则执行步骤(3)。

(3) 本端成员端口的属性类配置与聚合接口是否相同。

a. 执行 **display link-aggregation verbose** 命令查看本端处于 Unselected 状态的成员端口。

以二层聚合接口为例，Status 字段显示为“U”时，表示该成员处于 Unselected 状态：

```
<Sysname> display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 2a41-21c1-0100
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
  GE1/0/3             U        32768    3        2                      {AC}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    1        1        0x8000, 36f6-c0aa-0200 {ACDEF}
  GE1/0/2             32768    2        1        0x8000, 36f6-c0aa-0200 {ACDEF}
  GE1/0/3             32768    3        1        0x8000, 36f6-c0aa-0200 {AC}
```

b. 执行 **display current-configuration interface** 命令查看本端处于 Unselected 状态的成员端口的属性类配置（VLAN 等配置）与聚合接口是否相同，如果不同，则将其配置相同。

以如下显示为例，处于 Unselected 状态的成员端口 GigabitEthernet1/0/3 与参考端口 GigabitEthernet1/0/1 的属性类配置不同，导致该成员端口无法选中，需要修改成员端口 GigabitEthernet1/0/3 的属性类配置。

```
<Sysname> display current-configuration interface gigabitethernet 1/0/1
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 20
 port link-aggregation group 1
#
return
<Sysname> display current-configuration interface bridge-aggregation 1
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 to 100
 link-aggregation mode dynamic
#
return
```

如果本端成员端口的属性类配置与聚合接口相同，则执行步骤(4)。

(4) 本端成员端口的操作 key 与参考端口是否相同。

a. 执行 **display link-aggregation verbose** 命令查看本端处于 Unselected 状态的成员端口。

以三层聚合接口为例，Status 字段显示为“U”时，表示该成员处于 Unselected 状态：

```
<Sysname> display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
  GE1/0/3             U        32768    3        2                      {AC}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    1        1        0x8000, 36f6-c0aa-0200 {ACDEF}
  GE1/0/2             32768    2        1        0x8000, 36f6-c0aa-0200 {ACDEF}
  GE1/0/3             32768    3        1        0x8000, 36f6-c0aa-0200 {AC}
```

b. 执行 **display current-configuration interface** 命令查看本端处于 Unselected 状态的成员端口的操作 key（包括该端口的速率、双工模式等）与参考端口是否相同，如果不同，则将其配置相同。

以如下显示为例，处于 Unselected 状态的成员端口 GigabitEthernet1/0/3 与参考端口 GigabitEthernet1/0/1 的操作 key 不同，导致该成员端口无法选中，需要修改该端口速率配置。

```
<Sysname> display current-configuration interface gigabitethernet 1/0/1
#
interface GigabitEthernet1/0/1
 port link-mode route
 port link-aggregation group 11
#
return
<Sysname> display current-configuration interface gigabitethernet 1/0/3
#
interface GigabitEthernet1/0/3
 port link-mode route
 speed 100
 port link-aggregation group 11
#
return
```

如果本端成员端口的操作 key 与参考端口相同，则执行步骤(5)。

(5) 本端聚合接口是否为动态聚合。

如果是动态聚合，则执行步骤(6)；如果是静态聚合，否则进行步骤(8)。

(6) LACP 报文收发是否正确。

执行 **debugging link-aggregation lacp packet** 命令确认 LACP 报文收发是否正确。执行命该令后，查看成员端口 send 信息中 Actor 信息和 receive 信息中 Partner 信息。如果 sys-mac、key 和 port-index 字段的显示不一致，则 LACP 协议报文收发不正常，请排除收发光纤错接问题；如果 sys-mac、key 和 port-index 字段的显示一致，则 LACP 协议报文收发正常，请执行步骤(7)。

打开聚合组成员端口 GigabitEthernet1/0/1 的 LACP 报文调试信息开关，查看该端口收发 LACP 协议报文的情况。

```
<Sysname> debugging link-aggregation lacp packet all interface gigabitethernet 1/0/1
*Nov  2 15:51:21:15 2021 Sysname LAGG/7/Packet: PACKET.GigabitEthernet1/0/1.send.
 size=110, subtype =1, version=1
 Actor: type=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=0x1, pri=0x8000,
port-index=0x2, state=0xc5
 Partner: type=2, len=20, sys-pri=0x0, sys-mac=0000-0000-0000, key=0x0, pri=0x0,
port-index=0x0, state=0x32
 Collector: type=3, len=16, col-max-delay=0x0
 Terminator: type=0, len=0
*Nov  2 15:55:21:15 2021 Sysname LAGG/7/Packet: PACKET.GigabitEthernet1/0/1.receive.
size=110, subtype =1, version=1
 Actor: type=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc00-0000, key=0x1, pri=0x8000,
port-index=0x6, state=0xd
 Partner: type=2, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=0x1, pri=0x8000,
port-index=0x2, state=0xc5
 Collector: type=3, len=16, col-max-delay=0x0
 Terminator: type=0, len=0
```

(7) 本端成员端口的对端端口的操作 key 和属性类配置与参考端口的对端端口是否相同。

在本端 Unselected 端口的对端设备上执行 **display current-configuration interface** 命令查看对端 Unselected 端口的属操作 key 和属性类配置与参考端口的对端端口是否相同，如果不同，则将其配置相同。

如果本端成员端口的对端端口的操作 key 和属性类配置与参考端口的对端端口相同，则执行步骤(8)。

(8) 聚合成员端口数量是否达到阈值。

- 聚合成员端口数超过上限。

  可在聚合接口视图下通过 **link-aggregation selected-port maximum** 命令配置聚合组中的最大选中端口数。通过 **display link-aggregation verbose** 命令查看聚合组中成员端口数是否超过上限，如果超过上限，则多出来的端口为 Unselected 状态，Selected 端口按照端口编号从小到大排序。请在成员端口视图下使用 **undo port link-aggregation group** 命令将 Selected 端口中不适用的端口从聚合组中删除，以使必须使用的端口能够选中。

- 聚合成员端口数低于下限。

  可在聚合接口视图下执行 **link-aggregation selected-port minimum** 命令配置聚合组中的最小选中端口数。通过 **display link-aggregation verbose** 命令查看聚合组中成员端口是否低于下限，如果低于下限，则所有成员端口为 Unselected 状态。请执行 **link-aggregation selected-port minimum** 命令修改最小选中端口数值或者为聚合组添加成员端口，使其满足最小选中要求。

如果聚合成员端口数量未达到聚合组的阈值，则执行步骤(9)。

(9) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

8 二层技术-广域网接入类故障处理

8.1 PPP故障处理

8.1.1 PPP 接口协议 DOWN

1. 故障描述

当两台设备的 PPP 物理接口连接完成后，接口的链路层协议状态显示为 DOWN。

2. 常见原因

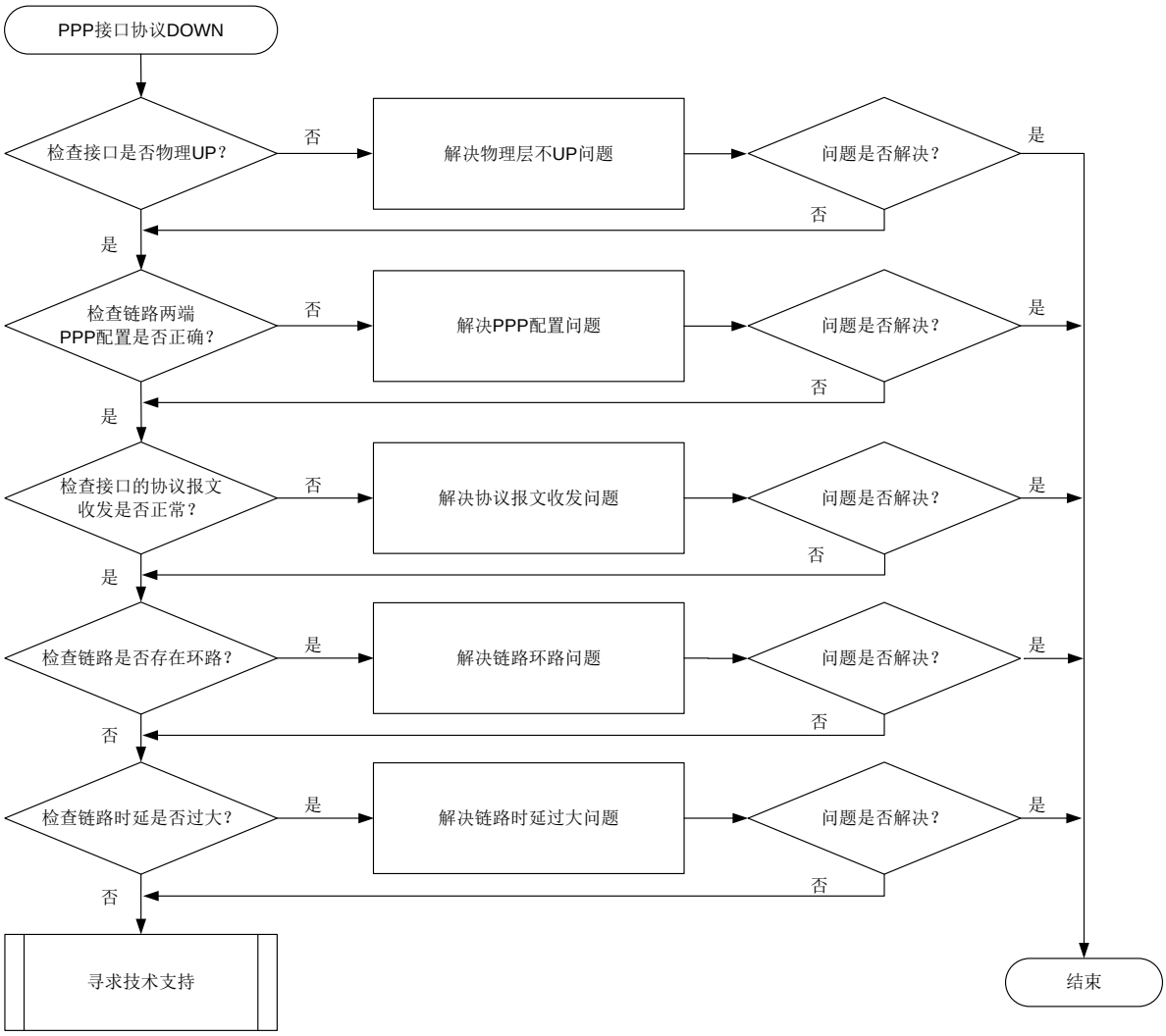
本类故障的常见原因主要包括：

- 接口的物理层状态没有 UP。
- 链路两端接口上的 PPP 相关配置错误。
- PPP 协议报文被丢弃。
- 链路存在环路。
- 链路时延过大。

3. 故障分析

本类故障的诊断流程如图 40 所示。

图40 PPP 接口协议 DOWN 的故障诊断流程图



4. 处理步骤

(1) 检查接口物理状态是否 UP。

在任意视图下执行 **display interface** *interface-type interface-number* 命令查看本端接口物理状态：

- 如果本端接口物理状态为 Administratively DOWN，表示本端接口被 **shutdown** 命令关闭，请在本端接口视图下执行 **undo shutdown** 命令取消关闭。

- 如果本端接口物理状态为 DOWN，请检查对端接口是否被 **shutdown** 命令关闭，如是，请在对端接口视图下执行 **undo shutdown** 命令取消关闭。
- 请检查两端光纤/光模块是否插好、光纤收/发是否插正确等，并解决接口物理状态 DOWN 问题。
- 如果接口状态为 UP，请继续执行下一步。

(2) 检查链路两端的 PPP 配置是否正确。

在 PPP 协议 DOWN 的接口所在视图下执行 **display this** 命令查看当前接口的 PPP 相关配置。

```
[Sysname-Serial2/1/0] display this
#
interface Serial2/1/0
 ip address 12.1.1.1 255.255.255.0
#
return
```

- 检查两端接口的链路层协议，确保两端接口配置的链路层协议都为 PPP，具体为：分别在两端设备任意视图下执行 **display interface** *interface-type interface-number* 命令查看两端接口的显示信息中“Link layer protocol”字段取值是否为“PPP”，若不是 PPP，请在相应接口视图下执行 **link-protocol ppp** 命令配置为 PPP。
- 如果配置了 PPP 认证，检查认证方与被认证方的认证类型、认证用户名/密码是否相同，如果不同，请参考 PPP 配置指导修改。
- 如果两端接口加入了 MP-group，请检查对应 MP-group 接口是否被 **shutdown** 命令关闭如是，请在 MP-group 接口视图下执行 **undo shutdown** 命令取消关闭。
- 如果一端接口配置了 **remote address** 命令，请确保另一端接口配置了 **ip address ppp-negotiate** 命令或通过 **ip address** 命令手工配置了对端 **remote address** 命令指定的 IP 地址。

如果 PPP 配置正确，但 PPP 接口协议仍为 DOWN，请继续执行下一步。

(3) 检查接口的协议报文收发是否正常。

在任意视图下执行 **display ppp packet statistics** 命令查看 PPP 协议报文的统计信息，并确认报文收发是否正常。

```
<Sysname> display ppp packet statistics slot 2
PPP packet statistics in slot 2:
----------------------------------LCP-------------------------------------
SEND_LCP_CON_REQ        : 4           RECV_LCP_CON_REQ        : 5
SEND_LCP_CON_NAK        : 0           RECV_LCP_CON_NAK        : 0
SEND_LCP_CON_REJ        : 0           RECV_LCP_CON_REJ        : 0
SEND_LCP_CON_ACK        : 4           RECV_LCP_CON_ACK        : 4
SEND_LCP_CODE_REJ       : 0           RECV_LCP_CODE_REJ       : 0
SEND_LCP_PROT_REJ       : 0           RECV_LCP_PROT_REJ       : 0
SEND_LCP_TERM_REQ       : 2           RECV_LCP_TERM_REQ       : 1
SEND_LCP_TERM_ACK       : 1           RECV_LCP_TERM_ACK       : 0
SEND_LCP_ECHO_REQ       : 25          RECV_LCP_ECHO_REQ       : 0
SEND_LCP_ECHO_REP       : 0           RECV_LCP_ECHO_REP       : 25
SEND_LCP_FAIL           : 0
```

```
----------------------------------IPCP-----------------------------------
SEND_IPCP_CON_REQ       : 38          RECV_IPCP_CON_REQ       : 2
SEND_IPCP_CON_NAK       : 0           RECV_IPCP_CON_NAK       : 0
SEND_IPCP_CON_REJ       : 0           RECV_IPCP_CON_REJ       : 0
SEND_IPCP_CON_ACK       : 2           RECV_IPCP_CON_ACK       : 2
SEND_IPCP_CODE_REJ      : 0           RECV_IPCP_CODE_REJ      : 0
SEND_IPCP_PROT_REJ      : 0           RECV_IPCP_PROT_REJ      : 0
SEND_IPCP_TERM_REQ      : 0           RECV_IPCP_TERM_REQ      : 0
SEND_IPCP_TERM_ACK      : 0           RECV_IPCP_TERM_ACK      : 0
SEND_IPCP_FAIL          : 0
---------------------------------IPV6CP----------------------------------
SEND_IPV6CP_CON_REQ     : 0           RECV_IPV6CP_CON_REQ     : 0
SEND_IPV6CP_CON_NAK     : 0           RECV_IPV6CP_CON_NAK     : 0
SEND_IPV6CP_CON_REJ     : 0           RECV_IPV6CP_CON_REJ     : 0
SEND_IPV6CP_CON_ACK     : 0           RECV_IPV6CP_CON_ACK     : 0
SEND_IPV6CP_CODE_REJ    : 0           RECV_IPV6CP_CODE_REJ    : 0
SEND_IPV6CP_PROT_REJ    : 0           RECV_IPV6CP_PROT_REJ    : 0
SEND_IPV6CP_TERM_REQ    : 0           RECV_IPV6CP_TERM_REQ    : 0
SEND_IPV6CP_TERM_ACK    : 0           RECV_IPV6CP_TERM_ACK    : 0
SEND_IPV6CP_FAIL        : 0
---------------------------------OSICP-----------------------------------
SEND_OSICP_CON_REQ      : 0           RECV_OSICP_CON_REQ      : 0
SEND_OSICP_CON_NAK      : 0           RECV_OSICP_CON_NAK      : 0
SEND_OSICP_CON_REJ      : 0           RECV_OSICP_CON_REJ      : 0
SEND_OSICP_CON_ACK      : 0           RECV_OSICP_CON_ACK      : 0
SEND_OSICP_CODE_REJ     : 0           RECV_OSICP_CODE_REJ     : 0
SEND_OSICP_PROT_REJ     : 0           RECV_OSICP_PROT_REJ     : 0
SEND_OSICP_TERM_REQ     : 0           RECV_OSICP_TERM_REQ     : 0
SEND_OSICP_TERM_ACK     : 0           RECV_OSICP_TERM_ACK     : 0
SEND_OSICP_FAIL         : 0
---------------------------------MPLSCP----------------------------------
SEND_MPLSCP_CON_REQ     : 0           RECV_MPLSCP_CON_REQ     : 0
SEND_MPLSCP_CON_NAK     : 0           RECV_MPLSCP_CON_NAK     : 0
SEND_MPLSCP_CON_REJ     : 0           RECV_MPLSCP_CON_REJ     : 0
SEND_MPLSCP_CON_ACK     : 0           RECV_MPLSCP_CON_ACK     : 0
SEND_MPLSCP_CODE_REJ    : 0           RECV_MPLSCP_CODE_REJ    : 0
SEND_MPLSCP_PROT_REJ    : 0           RECV_MPLSCP_PROT_REJ    : 0
SEND_MPLSCP_TERM_REQ    : 0           RECV_MPLSCP_TERM_REQ    : 0
SEND_MPLSCP_TERM_ACK    : 0           RECV_MPLSCP_TERM_ACK    : 0
SEND_MPLSCP_FAIL        : 0
---------------------------------AUTH------------------------------------
SEND_PAP_AUTH_REQ       : 0           RECV_PAP_AUTH_REQ       : 0
SEND_PAP_AUTH_ACK       : 0           RECV_PAP_AUTH_ACK       : 0
SEND_PAP_AUTH_NAK       : 0           RECV_PAP_AUTH_NAK       : 0
SEND_CHAP_AUTH_CHALLENGE: 0           RECV_CHAP_AUTH_CHALLENGE: 0
SEND_CHAP_AUTH_RESPONSE : 0           RECV_CHAP_AUTH_RESPONSE : 0
SEND_CHAP_AUTH_ACK      : 0           RECV_CHAP_AUTH_ACK      : 0
SEND_CHAP_AUTH_NAK      : 0           RECV_CHAP_AUTH_NAK      : 0
```

```
SEND_PAP_AUTH_FAIL      : 0           SEND_CHAP_AUTH_FAIL     : 0
```

- 如果接收或者发送的报文数量均为 0，或者多次执行本命令发现显示的接收或者发送报文个数没有增长，说明协议报文在传输过程中发送丢包，请检查接口/光纤/光模块是否故障，解决报文丢失问题。如问题无法解决，请执行步骤（6）。
- 如果报文收发正常，请继续执行下一步。

(4) 检测链路是否存在环路。

在本端设备用户视图下执行 **debugging ppp all interface** *interface-type interface-number* 命令打开 PPP 的报文调试开关，查看本端是否存在报文内容完全（如报文类型、报文 ID、MagicNumber 取值等）相同的收发报文：

```
*Apr 7 19:38:04:384 2022 Sysname PPP/7/FSM_PACKET_0: -MDC=1-Slot=2;
PPP Packet:
    Ser2/1/0(109) Output LCP(c021) Packet, PktLen 14
    Current State reqsent, code ConfReq(01), id 0, len 10
    MagicNumber(5), len 6, val c5 ae e7 03
*Apr 7 19:38:04:390 2022 Sysname PPP/7/FSM_PACKET_0: -MDC=1-Slot=2;
PPP Packet:
    Ser2/1/0(109) Input LCP(c021) Packet, PktLen 14
    Current State reqsent, code ConfReq(01), id 0, len 10
    MagicNumber(5), len 6, val c5 ae e7 03
```

- 若存在，则表示链路有环路，请确认环路产生原因（例如光纤连接错误），并消除环路。如问题无法解决，请执行步骤（6）。
- 若不存在，则表示链路无环路，请继续执行下一步。

(5) 检查链路时延是否过大。

在本端设备用户视图下执行 **debugging ppp all interface** *interface-type interface-number* 命令打开 PPP 的报文调试开关，查看 PPP 协商报文的发送时间戳和接收时间戳之间的时间间隔来确定链路时延：

```
*Apr 7 19:38:04:384 2022 Sysname PPP/7/FSM_PACKET_0: -MDC=1-Slot=2;
PPP Packet:
    Ser2/1/0(109) Output LCP(c021) Packet, PktLen 14
    Current State reqsent, code ConfReq(01), id 0, len 10
    MagicNumber(5), len 6, val c5 ae e7 03
*Apr 7 19:38:04:387 2022 Sysname PPP/7/FSM_PACKET_0: -MDC=1-Slot=2;
PPP Packet:
    Ser2/1/0(109) Input LCP(c021) Packet, PktLen 14
    Current State acksent, code ConfAck(02), id 0, len 10
    MagicNumber(5), len 6, val c5 ae e7 03
```

确认链路的时延是否大于当前接口所配置的 PPP 协议报文的协商超时时间间隔（由接口视图下的 **ppp timer negotiate** 命令配置，缺省时间间隔为 3 秒）。

- 如果链路的时延过大，请执行 **ppp timer negotiate** 命令适当调大配置值，或者更换相应的设备/链路后重新检测链路的时延，直到链路的时延小于前接口的 PPP 协议报文协商超时值。
- 如果链路的时延不大，请继续执行下一步。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。

- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

8.2 PPPoE故障处理

8.2.1 PPPoE 拨号偶尔出现认证失败

1. 故障描述

标准的 PPPoE 的组网，MSR 设备作为 PPPoE Server，cams 作为认证服务器。

使用过程中客户端认证失败。

携带了错误的用户名(系统中没有分配这样的用户名)：

- Host Len: 42 Name:a:2yZsyoBNb16F355VlFaYDJ6ZyNqx8cb::b052204
- Host Len: 9 Name:^^b052204

2. 故障处理步骤

(1) 排除 MSR 设备的处理问题

通过命令行 **debugging ppp all** 和 **debugging radius packet**，查看调试信息：

```
*Oct 22 14:00:07:012 2014 3640 PPP/7/PAP_PACKET_0:
  PPP Packet:
      Virtual-Access0 Input PAP(c023) Packet, PktLen 32
      State ServerListen, code Request(01), id 9, Len 28
0W'ZK5A9fd00001 16  Name:
      Pwd  Len:  *  Pwd :******
*Oct 22 14:00:07:012 2014 3640 PPP/7/PAP_EVENT_0:
  PPP Event:
      Virtual-Access0 PAP Receive Request Event
      State ServerListen
*Oct 22 14:00:07:013 2014 3640 PPP/7/PAP_STATE_0:
  PPP State Change:
      Virtual-Access0 PAP: ServerListen --> WaitAAA
*Oct 22 14:00:07:013 2014 3640 RADIUS/7/PACKET:
    User-Name="\r0W'ZK5A9fd00001"
    User-Password******
    Service-Type=Framed-User
    NAS-Identifier="3640"
    NAS-Port=4096
```

```
    NAS-Port-Type=Ethernet
    Calling-Station-Id="8c21-0a7e-71c5"
    Acct-Session-Id="00000005201410221400070000001e001  225"
    NAS-Port-Id="slot=65535;subslot=0;port=0;vlanid=0"
    H3c-Ip-Host-Addr="255.255.255.255 8c:21:0a:7e:71:c5"
    NAS-IP-Address=60.191.123.92
    H3c-Product-Id="H3C MSR36-40"
H3c-Nas-Startup-Timestamp=1413972953
….
*Oct 22 13:59:46:225 2014 3640 PPP/7/PAP_EVENT_0:
  PPP Event:
      Virtual-Access0 PAP Receive AAA Result Event
      State WaitAAA
*Oct 22 13:59:46:225 2014 3640 PPP/7/AUTH_ERROR_0:
  PPP Error:
      Virtual-Access0 PAP: Receive AAA reject message, authentication failed!
```

如 debug 信息可以看出 PPP 收到的用户名已经是错误的，则排除 MSR 设备问题。

(2) 排查家用小型路由器拨号方式

家用小型路由器的拨号模式一般使用自动拨号模式，首先会以正常拨号模式进行拨号，在拨号失败后，会使用各种特殊拨号模式尝试拨号，而一般的认证服务器不支持特殊模式拨号，所以出现大量认证失败信息。因此，当出现类似的问题后，需要排查家用小型路由器首次拨号失败的原因。

提示

家用小路由器使用特殊拨号模式会导致异常用户名，可不予关注。

3. 故障诊断命令

命令	说明
display pppoe-server session summary	显示PPPoE会话信息
debugging ppp lcp all	PPP LCP阶段调试信息开关
debugging ppp pap all	PPP PAP阶段调试信息开关
debugging ppp ipcp all	PPP IPCP阶段调试信息开关
debugging radius packet	Radius数据包调试信息开关

9 三层技术-IP 路由类故障处理

9.1 BGP故障处理

9.1.1 BGP 会话无法进入 Established 状态

1. 故障描述

本地路由器与对等体/对等体组建立的 BGP 会话无法进入 Established 状态。

2. 常见原因

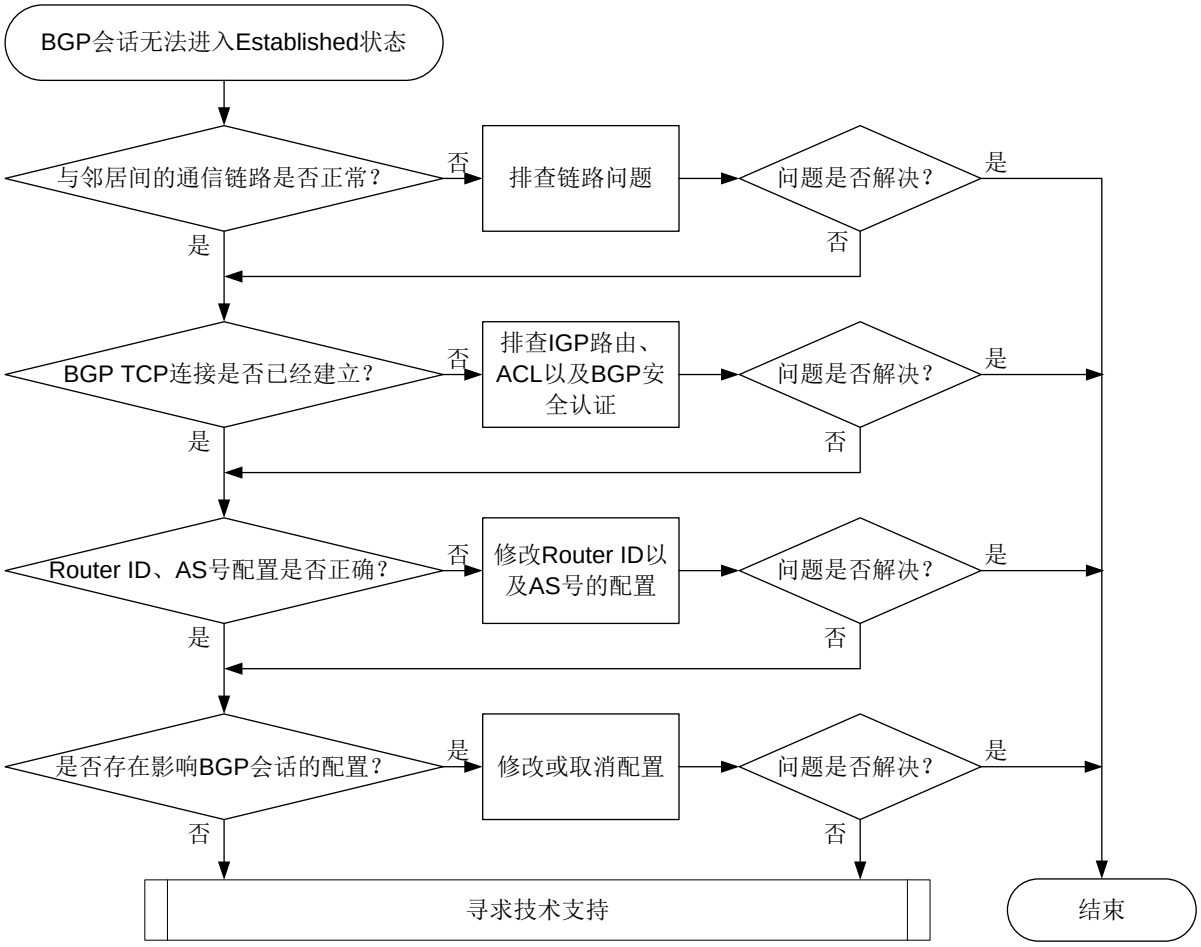
本类故障的常见原因主要包括：

- BGP 报文转发受阻。
- 建立/维持 BGP TCP 连接的报文被 ACL 过滤。
- 自治系统内，BGP 邻居间的 Router ID 产生冲突。
- 指定了错误的对等体/对等体组的 AS 号。
- 指定对等体的地址为 Loopback 接口的 IP 地址时，对端未通过 **peer connect-interface** 命令将建立 TCP 连接所使用的源接口配置为 Loopback 接口，或者对端未通过 **peer source-address** 命令将建立 TCP 连接所使用的源地址配置为 Loopback 接口的地址。
- 建立 BGP TCP 连接时，BGP 会话两端发送的 TCP 报文长度过大，在转发时被出接口 MTU 较小且无法对报文分片的中间节点丢弃，导致 BGP TCP 连接失败。
- 指定 EBGP 对等体的地址为 Loopback 接口的 IP 地址时，对端未配置 **peer ebgp-max-hop** 命令，以允许本地路由器同非直连邻居建立 EBGP 会话。
- BGP 会话的两端未通过 **peer password** 命令配置相同的密钥，导致 MD5 认证失败。
- 配置 **peer ttl-security** 命令以开启指定对等体/对等体组的 GTSM 功能时，到达对等体/对等体组的最大跳数配置错误，导致对等体/对等体组无法通过 GTSM 检查。
- 对等体向本地路由器发送的 BGP 路由数量超过了 **peer route-limit** 命令设定的最大值，导致 BGP 会话断开。
- BGP 路由器上配置了 **peer ignore**、**ignore all-peers** 或 **shutdown process** 命令，禁止建立 BGP 会话。
- 本地路由器与对端路由器没有在相同的地址族视图下使能路由信息交换能力。

3. 故障分析

本类故障的诊断流程如图 41 所示：

图41 BGP 会话无法进入 Established 状态的故障诊断流程图



4. 处理步骤

(1) 检查与 BGP 邻居之间的通信链路是否正常。

a. 检查与邻居建立 BGP 会话的相关接口是否处于 UP 状态。

b. 通过 **ping** 命令方式检查与 BGP 邻居的连通性。如果 Ping 的结果为可达，则说明本地路由器与 BGP 邻居之间的通信链路正常，请执行步骤（2）。如果 Ping 的结果为不可达，请执行步骤 c。

说明

建议使用 **ping -a** *source-ip* **-s** *packet-size* 命令和 **ping ipv6 -a** *source-ipv6* **-s** *packet-size* 命令来检测与 BGP 邻居的连通性。**-a** *source-ip* 和 **-a** *source-ipv6* 参数指定了 ICMP 回显请求报文的源地址，方便用户同时检测两端的链路是否都正常；**-s** *packet-size* 参数指定了发送的 ICMP 回显请求报文的长度，方便用户检测长报文在链路中的传输情况。Ping 操作的源 IP 地址取用本端建立 BGP 会话使用的接口的 IP 地址，目的 IP 地址取用对端建立 BGP 会话使用的接口的 IP 地址。

---

c. 执行 **ping -a** *source-ip* **-s** *packet-size* 命令进行 Ping 操作，并逐步减小**-s** *packet-size* 参数输入的值，当该参数减小到某个值时，Ping 的结果变为可达，则表示建立 BGP TCP 连接时发送的 TCP 报文由于长度过长，在转发过程中被设备丢弃，导致了 BGP 会话无法进入 Established 状态。

- 此时可以重复执行 **ping -a** *source-ip* **-s** *packet-size* 命令，调整**-s** *packet-size* 参数的取值，直至找到一个合适的取值（Ping 的结果为可达的前提下，取尽量大的值，以提高转发效率），然后将该值设置为 BGP 报文转发出接口的 MTU 值。可通过在接口上执行 **ip**/**ipv6 mtu** *mtu-size* 或 **tcp mss** *value* 命令，或者在 BGP 实例视图/BGP-VPN 实例视图下执行 **peer tcp-mss** 命令来设置出接口的 MTU 值；其中，**ip**/**ipv6 mtu** *mtu-size* 命令配置的是 MTU 值，**tcp mss** *value* 和 **peer tcp-mss** 命令配置的是 TCP MSS 值（TCP MSS＝MTU 值－IP 头部长度－TCP 头部长度）。
- 也可以无需重复进行 Ping 操作，直接在系统视图下执行 **tcp path-mtu-discovery** 命令，开启 TCP 连接的 Path MTU 探测功能。之后，设备会根据探测机制自动获得建立 TCP 连接的路径上最小的 MTU 值，并计算得到 MSS 值，后续建立 BGP TCP 连接时，会使用计算得到的 MSS 值作为 TCP 报文的长度。

如果无论怎么调整**-s** *packet-size* 参数的取值，Ping 的结果均为不可达，请参见“三层技术-IP 业务类故障处理”手册中的“Ping 不通的定位思路”进行后续的检查。

d. 如果故障仍不能排除，请执行步骤（2）

(2) 检查 BGP TCP 连接是否建立。

执行 **display tcp** 命令，查看显示信息中是否存在地址为本地路由器地址以及 BGP 邻居的地址、对端端口号为 179、TCP 连接状态为 ESTABLISHED 的条目。例如：

```
<Sysname> display tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       PCB
 0.0.0.0:179           12.1.1.2:0            LISTEN      0xfffffffffffff9d
 12.1.1.1:28160        12.1.1.2:179          ESTABLISHED 0xfffffffffffff9e
```

如果存在，则执行步骤（3）；如果不存在，则进行以下检查：

- 执行 **display ip routing-table** 或 **display ipv6 routing-table** 命令，查看路由表中是否存在对端建立 BGP 会话使用的 IPv4/IPv6 地址的 IGP 路由，如果不存在，请检查 IGP 路由的配置。常见的 IGP 路由协议故障处理方法，请参见“三层技术-IP 路由类故障处理”手册中的“OSPF 故障处理”、“OSPFv3 故障处理”或“IS-IS 故障处理”。
- 执行 **display acl all** 命令，查看是否存在拒绝端口号为 bgp 的规则，例如：

  ```
  <Sysname> display acl all
  Advanced IPv4 ACL 3077, 2 rules,
  ACL's step is 5
   rule 1 deny tcp destination-port eq bgp
   rule 2 deny tcp source-port eq bgp
  ```

  如果存在这样的规则，请执行 **undo rule** 命令取消这些配置。
- 执行 **debugging tcp packet** 命令，根据 Debug 信息判断 BGP 建立 TCP 连接时是否存在安全认证失败，例如：

  ```
  <Sysname> debugging tcp packet acl 3000
  *Feb  5 20:03:39:289 2021 Sysname SOCKET/7/INET: -MDC=1;
  ```

```
TCP Input: Failed to check md5, drop the packet.
```

上述信息表明 BGP 建立 TCP 连接时 MD5 认证失败。请在建立 BGP TCP 连接的两端设备上均执行 **peer password** 命令配置相同的密钥。

```
<Sysname> debugging tcp packet acl 3000
*Feb  5 20:03:39:289 2021 Sysname SOCKET/7/INET: -MDC=1;
TCP Input: Failed to check keychain, drop the packet.
```

上述信息表明 BGP 建立 TCP 连接时 keychain 认证失败。请确保建立 BGP TCP 连接的两端设备上均通过执行 **peer keychain** 命令配置了 keychain 认证，并且同一时间内使用的 key 的标识符相同，以及相同标识符的 key 的认证算法和认证密钥一致。

```
<Sysname> debugging tcp packet acl 3000
*Feb  5 20:03:39:289 2021 Sysname SOCKET/7/INET: -MDC=1;
TCP Input: Failed to get IPSEC profile, index 500, name profile1(inpcb profile2),
return 0x3fff.
```

上述信息表明 BGP 建立 TCP 连接时 IPsec 认证失败。请检查 BGP 会话两端设备的 IPsec 配置并确保在两端设备上均通过执行 **peer ipsec-profile** 命令应用了 IPsec 安全框架。

如果故障仍不能排除，请执行步骤（3）。

(3) 检查 Router ID 是否存在冲突，AS 号是否配置错误。

a. 执行 **display bgp peer** 命令，根据显示信息中的“BGP local router ID”字段，判断是否存在 Router ID 配置冲突，如果存在冲突，请在需要建立 BGP 会话的 BGP 实例视图或 BGP-VPN 实例视图下执行 **router-id** 命令，修改 BGP 路由器的 Router ID。例如：

```
<Sysname> display bgp peer ipv4 unicast

 BGP local router ID: 12.1.1.1
 Local AS number: 10
 Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State

 12.1.1.2                20        3        3    0        0 00:00:25 Established
```

b. 执行 **display bgp peer** 命令，根据显示信息中的“AS”字段，判断是否为 BGP 对等体/对等体组指定了错误的 AS 号。如果 AS 号配置错误，则执行 **peer as-number** 命令为 BGP 对等体/对等体组指定正确的 AS 号。例如：

```
<Sysname> display bgp peer ipv4 unicast

 BGP local router ID: 12.1.1.1
 Local AS number: 10
 Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State

 12.1.1.2                20        3        3    0        0 00:00:25 Established
```

c. 如果故障仍不能排除，请执行步骤（4）。

(4) 在 BGP 实例视图下执行 display this 命令，检查是否存在影响 BGP 会话的配置。

表3 影响 BGP 会话的配置检查项

检查项	描述
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **connect-interface** *interface-type interface-number*	本端存在该配置时，BGP邻居也需要使用Loopback接口的地址建立BGP会话，可通过本命令或**peer source-address**命令配置
peer *ipv4-address* [*mask-length*] **source-address** *source-ipv4-address* **peer** *ipv6-address* [*prefix-length*] **source-address** *source-ipv6-address*	本端存在该配置时，BGP邻居也需要使用Loopback接口的地址建立BGP会话，可通过本命令或**peer connect-interface**命令配置
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ebgp-max-hop** [*hop-count*]	非直连网络上的邻居建立EBGP会话，或者直连网络设备使用Loopback接口建立EBGP会话时，BGP会话两端均需要配置本命令，为EBGP会话指定相应的最大跳数
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ttl-security hops** *hop-count*	存在该配置时，本地路由器从指定对等体收到的BGP报文中，TTL需要在255-“*hop-count*”+1到255之间，否则BGP报文将会被丢弃，如果本地路由器与对等体之间的跳数超过了*hop-count*，请通过本命令进行配置修改
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] | *link-local-address* **interface** *interface-type interface-number* } **route-limit** *prefix-number* [**reconnect** *reconnect-time* | *percentage-value*] *	存在该配置时，表示如果本地路由器从指定对等体/对等体组接收的路由数量大于*prefix-number*值，路由器会自动断开与指定对等体/对等体组的会话。可通过降低对等体/对等体组发送的路由数量，或配置更大的*prefix-number*值，来避免BGP会话断开
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **ignore**	存在该配置时，BGP将不会与指定的对等体/对等体组建立BGP会话，此时可以通过执行**undo peer ignore**命令允许建立与对等体/对等体组的会话
地址族下的**peer enable**命令	建立BGP会话时，两端需要在同一个地址族下指定对端配置**peer enable**命令使能路由信息交互能力。存在该配置时，请检查对端是否也在相同地址族下配置了**peer enable**命令

如果故障仍不能排除，请执行步骤（5）。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

在系统视图下执行 **snmp-agent trap enable bgp** 命令后，BGP 会话的状态机发生变化时会产生如下告警信息。

模块名：BGP4-MIB

- bgpBackwardTransition (1.3.6.1.2.1.15.7.2)

相关日志

无

9.1.2 BGP 会话 Down

1. 故障描述

在设备上观察到 BGP/5/BGP_STATE_CHANGED 提示 BGP 会话状态变为 Idle 的日志打印信息，会话状态从 Established 变为 Idle。

2. 常见原因

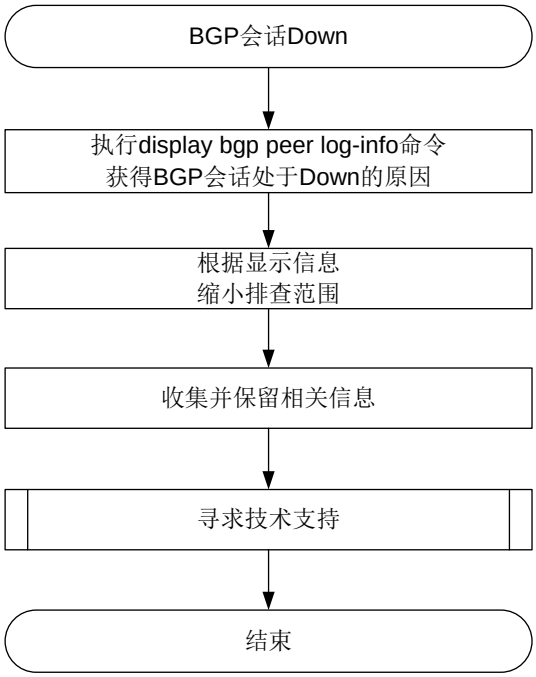
本类故障的常见原因主要包括：

- Keepalive 或 Update 消息收发超时。
- TCP 连接建立失败。
- 设备达到内存门限。
- BGP 报文解析发生错误。

3. 故障分析

本类故障的诊断流程如图 42 所示。

图42 BGP 会话 Down 的故障诊断流程图



4. 处理步骤

执行 **display bgp peer log-info** 命令，根据该命令的显示信息进一步确认 BGP 会话 Down 的原因。几种常见的 BGP 会话 Down 的原因如下：

- BGP 定时器超时导致断开会话

  如果 log-info 信息与下面的显示信息相似：

```
<Sysname> display bgp peer ipv4 3.3.3.3 log-info

 Peer: 3.3.3.3
```

```
    Date      Time    State Notification
                            Error/SubError

  17-Jan-2022 14:48:34 Down  Receive notification with error 4/0
                             Hold Timer Expired/ErrSubCode Unspecified
                             Keepalive last triggered time: 14:48:31-2022.1.17
                             Keepalive last sent time     : 14:48:31-2022.1.17
                             Update last sent time        : 14:48:24-2022.1.17
                             EPOLLOUT last occurred time  : 14:48:30-2022.1.17
```

则表示 BGP 会话 Down 的原因是在会话保持时间内未能收到对等体发送的 Keepalive 或 Update 消息。在 BGP 会话保持定时器超时后，设备则会主动断开 BGP 会话，并向对端对等体发送 Notification 消息。

定时器超时的原因可能是设备正常发送了 Keepalive 或 Update 消息，但报文由于链路故障等原因无法到达对等体或对等体处理不及时，或者设备调度故障导致未能及时产生 Keepalive 或 Update 消息等。如需解决此问题，请在 BGP 会话的两端设备的 Probe 视图下，均执行 **display system internal bgp log** 命令，并收集该命令的显示信息，联系技术支持人员进行进一步分析。

- TCP 连接错误导致 BGP 会话断开

  如果 log-info 信息与下面的显示信息相似：

```
<Sysname> display bgp peer ipv4 1.1.1.1 log-info

 Peer: 1.1.1.1

    Date      Time    State Notification
                            Error/SubError

  17-Jan-2022 14:42:01 Down  Receive TCP_Connection_Failed event
```

  则 BGP 会话 Down 的原因是 TCP 连接错误。BGP 使用 TCP 作为其传输层协议，如果 BGP 会话两端设备间的 TCP 连接发生错误，BGP 会话也会断开。如果用户观察到的显示信息与上述举例不相似，但是显示信息中包含了 Notification 消息错误码 5/0，则也是由于 TCP 连接错误导致的 BGP 会话断开。

  确认 TCP 连接发生错误后，请在 BGP 会话 Down 的两端设备的 Probe 视图中，均执行 **view /proc/tcp/tcp_log slot** *x* 命令（所有的单板/成员设备各执行一次），并收集该命令的显示信息，联系技术支持人员进行进一步分析。

- 内存不足导致 BGP 会话断开

  如果 log-info 信息与下面的显示信息相似：

```
<Sysname> display bgp peer ipv4 1.1.1.1 log-info
 Peer: 1.1.1.1
    Date      Time    State Notification
                            Error/SubError

  17-Jan-2022 15:38:53 Down  Send notification with error 6/8
                             Entered severe memory state
  17-Jan-2022 14:53:51 Down  Send notification with error 6/8
                             No memory to process the attribute
```

表明设备没有足够内存处理 BGP 模块相关功能，导致 BGP 会话断开。此类错误原因对应 log-info 信息中的错误码 6/8。

此时请在 BGP 会话 Down 的两端设备上，均执行 **display memory-threshold** 命令，获取内存告警门限相关信息，并记录 **display bgp peer log-info** 命令的显示信息，联系技术支持人员进行进一步分析。

- 报文解析错误导致 BGP 会话断开：

  BGP 会话两端的设备如果报文解析能力不同或版本不匹配，则 BGP 可能无法解析接收到的报文，导致 BGP 会话断开。此类错误原因对应 log-info 信息中的消息差错码 1、2 和 3（即“Error/SubError”中的“Error”为 1、2 或 3）。

  请在 BGP 会话 Down 的两端设备上，均执行 **debugging bgp raw-packet**、**debugging bgp open** 以及 **debugging bgp update** 命令，并收集这些命令的显示信息以及 **display bgp peer log-info** 命令的显示信息，联系技术支持人员进行进一步分析。

- 如果 **display bgp peer log-info** 命令的显示信息中，提示的 BGP 会话 Down 的原因不属于以上任何一种常见的原因，请收集如下信息，并联系技术支持人员。
  - **display bgp peer log-info** 命令的显示信息。
  - **display system internal bgp log** 命令的显示信息。
  - **view /proc/tcp/tcp_log slot** *x* 命令的显示信息（所有的单板/成员设备各执行一次）。
  - 设备的配置文件、日志信息、告警信息。

作为参考，BGP 会话断开的详细原因及其对应的错误码如表 4 所示。

表4 邻居断开的详细原因列表

差错码/差错子码	会话断开的详细原因	说明
1/1	connection not synchronized	连接不同步，目前实现为收到的报文的报文头前16字节不全为F
1/2	bad message length	报文长度无效
1/3	bad message type	报文的类型无效
3/1	the withdrawn length is too large	撤销信息长度过长
	the attribute length is too large	属性长度过长
	one attribute appears more than once	同一个属性在一个Update消息中出现了多次
	the attribute length is too small	属性长度字段不足2字节
	exntended length field is less than two octets	属性长度为可扩展长度，但长度字段不足2字节
	the length field is less than one octet	属性长度为正常长度，但长度字段不足1字节
	link-state attribute error	链路状态属性形式错误
3/2	unrecognized well-known attribute	不支持的公认属性
3/3	*attribute-type* attribute missed	*attribute-type*类型的属性丢失，*attribute-type*取值包括：

差错码/差错子码	会话断开的详细原因	说明
		• ORIGIN • AS_PATH • LOCAL_PREF • NEXT_HOP
3/4	attribute flags error	属性标记错误
3/5	*attribute-type* attribute length error	*attribute-type*类型的属性长度错误，*attribute-type*取值包括： • AS_PATH • AS4_PATH • CLUSTER_LIST • AGGREGATOR • AS4_AGGREGATOR • ORIGIN • NEXT_HOP • MED • LOCAL_PREF • ATOMIC_AGGREGATE • ORIGINATOR_ID • MP_REACH_NLRI • COMMUNITIES • extended communities
	attribute length exceeds	属性长度越界
3/6	invalid ORIGIN attribute	ORIGIN属性无效
3/8	invalid NEXT_HOP attribute	下一跳属性无效
3/9	invalid nexthop length in MP_REACH_NLRI (*address-family*)	*address-family*地址族MP_REACH_NLRI属性的Nexthop长度错误，*address-family*的取值包括： • 4u：表示 IPv4 单播地址族 • IPv4 Flowspec：表示 IPv4 Flowspec 地址族 • MPLS：表示 MPLS 地址族 • VPNv4：表示 VPNv4 地址族 • 6u：表示 IPv6 单播地址族 • VPNv6：表示 VPNv6 地址族 • L2VPN：表示 L2VPN 地址族
	the length of MP_UNREACH_NLRI is too small	MP_UNREACH_NLRI的长度小于3字节
	the MP NLRI attribute length exceeds	MP_REACH_NLRI 或MP_UNREACH_NLRI属性长度越界
	erroneous MP NLRI attribute end position	可达或不可达前缀结束位置与报文属性结

差错码/差错子码	会话断开的详细原因	说明
		束位置不同
3/10	invalid network field	网络字段无效
3/11	malformed AS_PATH	AS路径形式不对
4/0	Keepalive last triggered time	最后一次触发发送Keepalive消息时间
	Keepalive last sent time	最后一次发送Keepalive消息时间
	Update last sent time	最后一次发送Update消息时间
	EPOLLOUT last occurred time	最后一次发生EPOLLOUT时间
	Keepalive last received time	最后一次接收Keepalive消息时间
	Update last received time	最后一次接收Update消息时间
	EPOLLIN last occurred time	最后一次发生EPOLLIN时间
5/0	connection retry timer expires	ConnectRetry定时器超时
	TCP_CR_Acked event received	收到了TCP_CR_Acked事件
	TCP_Connection_Confirmed event received	收到了TCP_Connection_Confirmed事件
5/3	open message received	收到open消息
6/0	manualstop event received	收到manualstop事件
	physical interface configuration changed	物理配置改变，比如接口变化
	session down event received from BFD	收到BFD会话down事件
6/1	maximum number of prefixes reached	前缀数超过**peer route-limit**所配置的数目
	maximum number of *address-family* prefixes reached	*address-family*地址族的前缀数超过**peer route-limit**所配置的数目，*address-family*的取值包括： • IPv4 unicast：表示 IPv4 单播地址族 • IPv6 unicast：表示 IPv6 单播地址族 • VPNv4：表示 VPNv4 地址族 • VPNv6：表示 VPNv6 地址族
6/2	configuration of peer ignore changed	配置**peer ignore**命令
6/3	address family deleted	地址族被删除
	peer disabled	关闭对等体
6/4	administrative reset	执行**reset bgp**命令或者配置改变导致BGP会话重启
6/5	connection rejected	连接被拒绝
6/6	other configuration change	其他配置变化
6/7	connection collision resolution	连接冲突
	two connections exist and MD5 authentication	存在两个连接，且其中一个配置了MD5认

差错码/差错子码	会话断开的详细原因	说明
	is configured for the neighbor	证
6/8	• no memory to process the attribute：解析属性时内存不够 • no memory for the route：生成路由或者标签块信息时，获取不到内存 • no memory to generate unreachable NLRI：封装 unreachable NLRI 时申请不到内存 • no memory to generate a message：封装报文时申请不到内存 • can’t get the VPN RD：解析前缀时获取不到 RD • can’t get the VPN routing table：解析前缀时获取不到 VPN 路由表 • can’t get the attributes：解析前缀时获取不到属性 • entered severe memory state：进入二级门限告警 • entered critical memory state：进入三级门限告警	

5. 告警与日志

相关告警

无

相关日志

- BGP/5/BGP_STATE_CHANGED

9.2 IS-IS故障处理

9.2.1 IS-IS 邻居无法建立

1. 故障描述

- IS-IS 邻居 Down。
- IS-IS 邻居关系震荡。

2. 常见原因

本类故障的常见原因主要包括：

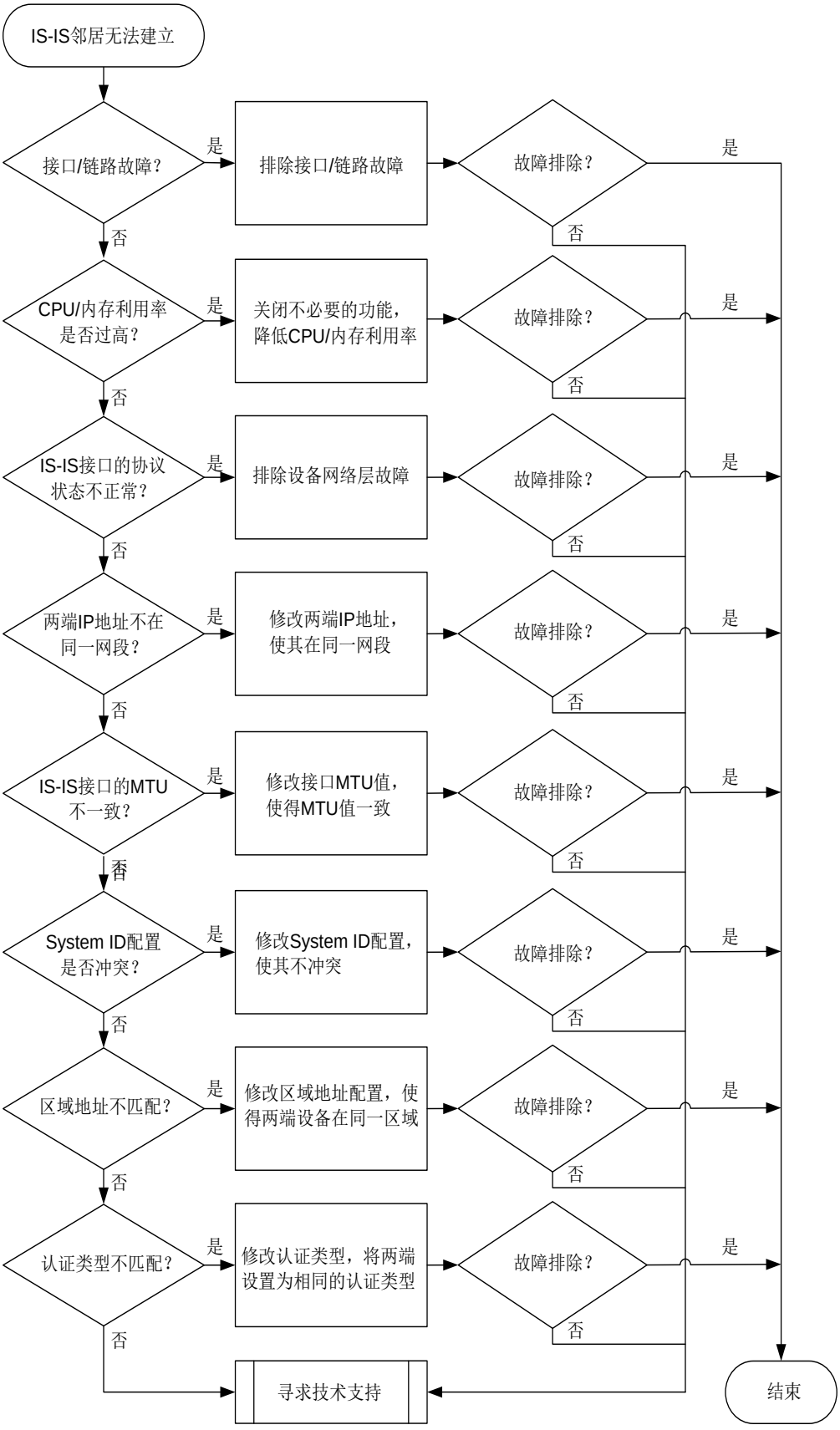
- 设备底层故障或者链路故障，导致 IS-IS 无法正常的收发 Hello 报文。
- 链路两端的设备配置的 System ID 相同。
- 链路两端接口的 MTU 设置不一致，或者接口的 MTU 小于发送的 Hello 报文的长度。
- 链路两端接口的 IP 地址不在同一网段。
- 链路两端的 IS-IS 接口认证方式不匹配。
- 链路两端的 IS-IS Level 不匹配。

- 建立 IS-IS Level-1 邻居时，链路两端设备的区域地址不匹配。

3. 故障分析

本类故障的诊断流程如图 43 所示。

图43 IS-IS 邻居无法建立的故障诊断流程图



4. 处理步骤

(1) 检查接口的物理层状态是否为 Up。

请执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看 IS-IS 接口物理层状态，如果接口物理层状态为 Down，请先处理接口故障问题。如果接口物理状态为 Up，请执行步骤(2)。

(2) 检查链路是否故障。

请执行 **ping** 命令，检查设备链路是否故障（包括传输设备故障）。如果链路正常，请执行步骤(3)。

如果 IS-IS 使用 BFD 检测设备间链路，通过 **isis bfd session-restrict-adj** 命令开启 BFD 抑制 IS-IS 建立和保持邻接关系的功能后，接口发送的 Hello 报文中将会携带 BFD-enabled TLV，当两端 BFD-enabled TLV 中的信息一致时，抑制 IS-IS 建立和保持邻居关系的功能生效。当 BFD 会话 Down 时，无法建立 IS-IS 邻居关系。

请执行 **display bfd session** 命令查看检测 IS-IS 两端链路的 BFD 会话的状态，如果“State”字段取值为“Down”，请排除链路故障。如果“State”字段取值为“Up”，请执行步骤(3)。

(3) 检查 CPU 或内存利用率是否过高。

请执行 **display cpu-usage** 命令检查故障设备的主控板和接口板的 CPU 利用率是否过高。如果 CPU 利用率过高，IS-IS 将无法正常收发协议报文，从而导致邻居关系震荡。可通过关闭一些不必要的功能解决此问题。如果 CPU 利用率不高，则执行步骤(4)。

请执行 **display memory-threshold** 命令，查看显示信息中的 Current free-memory state，即系统当前内存使用状态。如果 Current free-memory state 为 Minor、Severe 或 Critical，表示剩余空闲内存较少，可能会导致设备无法收发 IS-IS 报文或处理 IS-IS 报文速度较慢，请关闭一些不必要的功能尝试解决此问题。如果系统当前内存使用状态为 Normal，则执行步骤(4)。

(4) 检查接口在 IS-IS 协议下的状态是否正常。

请执行 **display isis interface** 命令，检查使能了 IS-IS 的接口的状态（“IPv4 state”或“IPv6 state”字段）是否为正常状态。

- 如果 IS-IS 接口状态为“Lnk:Up/IP:Dn”，说明 IPv4 或 IPv6 相邻节点的链路层可达、网络层不可达，请处理网络层故障问题。
- 如果 IS-IS 接口状态为“Up”，请执行步骤(5)。

(5) 检查两端 IP 地址是否在同一网段。

对于 IPv4 IS-IS，请执行 **display interface brief** 命令查看两端接口的 IPv4 地址。

- 如果两端接口的 IPv4 地址不在同一网段，请在接口视图下执行 **ip address** 命令修改两端的 IPv4 地址，使其在同一网段。
- 如果两端接口的 IPv4 地址处于同一网段，请执行(6)。

对于 IPv6 IS-IS，无需执行此检查。

(6) 检查各 IS-IS 接口的 MTU 是否一致。

请执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看接口 MTU 信息。

- 如果接口的 MTU 值配置不一致，请在接口视图下执行 **mtu** *size* 命令，将各个接口的 MTU 值修改为一致。

- 如果接口的 MTU 值一致，请执行(7)。

(7) 检查链路两端的设备配置的 System ID 是否相同。

请执行 **display current-configuration isis** 命令检查链路两端的设备配置的 System ID 是否相同。

- 如果两端 System ID 相同，请修改配置，使两端的 System ID 不同。
- 如果两端 System ID 不相同，请执行步骤(8)。

(8) 检查链路两端的设备的 IS-IS Level 是否匹配。

请检查设备及 IS-IS 接口的 Level 级别：

- 请执行 **display current-configuration | include is-level** 命令，检查链路两端设备的 Level 级别。如果通过 **display current-configuration | include is-level** 命令无法查询到设备的 Level 级别的相关配置，表明设备的 Level 级别为缺省值为 Level-1-2。
- 请执行 **display current-configuration interface** *interface-type interface-number* **| include circuit-level** 命令，检查接口的链路邻接关系类型。如果通过 **display current-configuration interface** *interface-type interface-number* **| include circuit-level** 命令无法查询到接口的链路邻接关系类型，说明接口的链路邻接关系类型为缺省值，这种情况下，该接口既可以建立 Level-1 的邻接关系，也可以建立 Level-2 的邻接关系。

需要保证链路两端的 Level 匹配才能建立 IS-IS 邻居关系，接口 Level 匹配的原则如下：

- 如果本端接口 Level 级别为 Level-1，则对端接口 Level 级别必须为 Level-1 或 Level-1-2。
- 如果本端接口 Level 级别为 Level-2，则对端接口 Level 级别必须为 Level-2 或 Level-1-2。
- 如果本端接口 Level 级别为 Level-1-2，则对端接口 Level 级别可以为 Level-1、Level-2 或 Level-1-2。

对于不同的情况，请选择不同的处理方式：

- 如果链路两端设备的 IS-IS Level 不匹配，请在 IS-IS 视图下使用 **is-level** 命令修改设备的 IS-IS 级别，或者在接口视图下使用 **isis circuit-level** 命令修改接口的 Level 级别。
- 如果链路两端设备的 IS-IS Level 匹配，请执行步骤(9)。

(9) 检查链路两端设备的区域地址是否匹配。

请执行 **display isis** 命令查看“Network entity”字段，检查链路两端设备的区域地址是否匹配。“Network entity”的格式为 X…X.XXXX.XXXX.XXXX.00，前面的“X…X”是区域地址，中间的 12 个“X”是交换机的 System ID，最后的“00”是 SEL。

- 如果链路两端建立 Level-1 邻居，需要保证链路两端设备在同一个区域内。建立 IS-IS Level-2 邻居时，不需要判断区域地址是否匹配。

  当建立 Level-1 邻居的两端设备区域地址不同时，请在 IS-IS 视图下使用 **network-entity** 命令修改设备的区域地址。
- 如果链路两端区域地址匹配，请执行步骤(10)。

(10) 检查链路两端设备的认证方式是否匹配。

请执行 **display current-configuration** *interface-type interface-number* **| include isis** 命令检查链路两端设备 IS-IS 接口的认证方式。

a. 如果两端认证类型不匹配，请在链路两端设备的 IS-IS 接口视图下执行 **isis authentication-mode** 命令，将两端设置为相同的认证类型。
b. 如果认证方式相同的情况下，IS-IS 仍然无法建立邻居关系，请将两端设置为相同的认证密码。

如果故障依然存在，请执行步骤(11)。

(11) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：ISIS-MIB

- isisAdjacencyChange (1.3.6.1.2.1.138.0.17)

相关日志

- ISIS/3/ISIS_NBR_CHG

9.2.2 设备学习不到 IS-IS 路由

1. 故障描述

设备学习不到 IS-IS 路由。

2. 常见原因

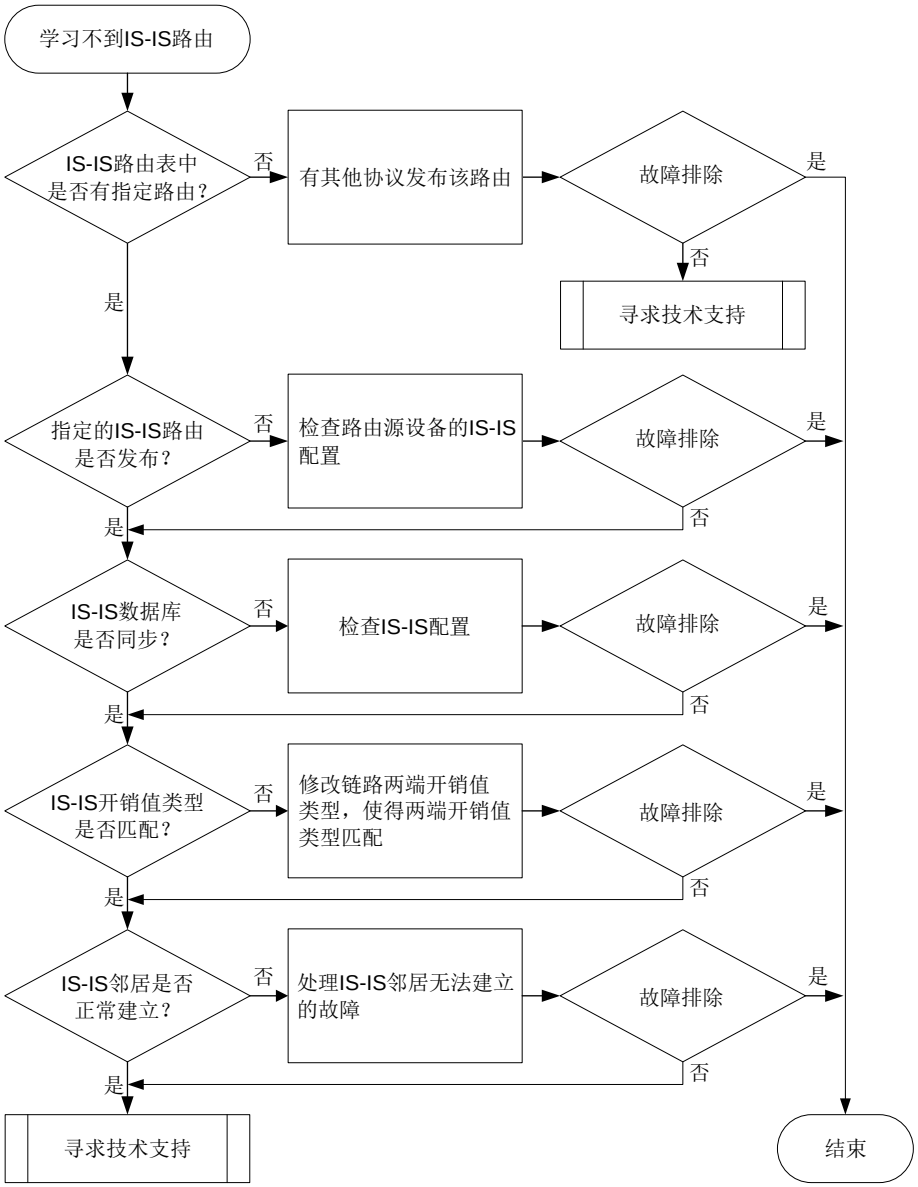
本类故障的常见原因主要包括：

- 其它路由协议也发布了相同的路由，并且路由协议优先级比 IS-IS 协议高。
- 引入的外部路由优先级低，没有被优选。
- IS-IS 开销值类型不匹配。
- IS-IS 邻居没有正常建立。
- 两台设备的 System ID 配置相同。
- LSP 报文认证不匹配。
- 设备底层故障或者链路故障，造成 LSP 报文丢失。
- LSP 长度超过了设备可以接收的 LSP 的最大长度。

3. 故障分析

本类故障的诊断流程如图 44 所示。

图44 设备学习不到 IS-IS 路由的故障诊断流程图



4. 处理步骤

(1) 检查 IS-IS 路由表是否正确。

请执行 **display isis route** 命令，查看 IS-IS 路由表。

- 如果 IS-IS 路由表中存在指定的路由，请执行 **display ip routing-table ip-address** [*mask* | *mask-length*] **verbose** 命令查看 IP 路由表中是否存在协议优先级比 IS-IS 高的路由。
  - 如果存在，请根据网络规划调整配置。
  - 如果不存在，请执行步骤(6)。
- 如果 IS-IS 路由表中不存在指定的路由，请执行步骤(2)。

(2) 检查指定的 IS-IS 路由是否发布。

在发布指定路由的设备上，执行 **display isis lsdb verbose local** 命令，查看本地产生的 LSP 报文中是否携带了指定路由。

- 如果 LSP 报文中没有携带指定的路由，请检查 IS-IS 配置是否正确，例如接口是否使能 IS-IS。如果指定的路由是 IS-IS 引入的外部路由，请执行 **display ip routing-table protocol** *protocol* **verbose** 命令查看该路由的“State”字段，当“State”字段的取值中包含“Inactive”时，说明外部路由处于非激活状态，这种情况下，IS-IS 不会将此路由发布出去。请检查外部路由的配置，使该路由的“State”取值包含“Active”和“Adv”。
- 如果 LSP 报文中携带了指定的路由，请执行步骤(6)。

(3) 检查 IS-IS 的数据库是否同步。

在学习不到 IS-IS 路由的设备上，执行 **display isis lsdb** 命令，查看是否收到发布指定路由的设备的 LSP 报文。

- 如果 LSDB 数据库中不存在指定的 LSP 报文，请排查是否存在链路故障。如果不存在链路故障，请通过 **display isis** 命令查看“LSP length receive”字段的取值，判断指定的 LSP 报文长度是否超过了设备可以接收的 LSP 报文的最大长度。当“LSP length receive”字段的取值超过了设备可以接收的 LSP 报文的最大长度时，请在生成 LSP 的设备上通过 **lsp-length originate** 命令将生成 LSP 报文的最大长度配置为该区域内所有 IS-IS 接口 MTU 的最小值。
- 如果 LSDB 数据库中存在指定的 LSP 报文，但 Seq Num 与发布该 LSP 的设备上通过 **display isis lsdb local verbose** 命令显示的 Seq Num 不一致，并且 Seq Num 在不停地增长，则网络中存在其他设备与发布指定路由的设备的 System ID 配置相同，请排查并修改网络中设备的 System ID 配置。
- 如果 LSDB 数据库中存在指定的 LSP 报文，但 Seq Num 与发布该 LSP 的设备上通过 **display isis lsdb local verbose** 命令显示的 Seq Num 不一致，并且一直保持不变，可能是 LSP 报文在传输过程中被丢弃，请排查设备底层和中间链路是否存在故障。
- 如果 LSDB 数据库中存在指定的 LSP 报文，并且 Seq Num 与发布该 LSP 的设备上通过 **display isis lsdb local verbose** 命令显示的 Seq Num 一致，请执行步骤(6)。

(4) 检查 IS-IS 开销值类型是否匹配。

分别在发布路由的设备和学习不到路由的设备上，执行 **display isis** 命令，查看“Cost style”的取值，检查两端的 IS-IS 开销值类型是否匹配。只有开销值类型相同时，才能学到路由。

- 如果链路两端设备的 IS-IS 开销值类型不匹配，请在 IS-IS 视图下执行 **cost-style** 命令修改配置。
- 如果两端设备的 IS-IS 开销值类型匹配，请执行步骤(6)。

(5) 检查 IS-IS 邻居是否正常建立。

在路径上的每一台设备上执行 **display isis peer** 命令，查看 IS-IS 邻居是否都正常建立。

- 如果存在邻居没有正常建立的情况，请参见“9.2.1 IS-IS 邻居无法建立”。
- 如果不存在邻居未能正常建立的情况，请执行步骤(6)。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

9.2.3 IS-IS 路由震荡

1. 故障描述

IS-IS 路由反复增删。

2. 常见原因

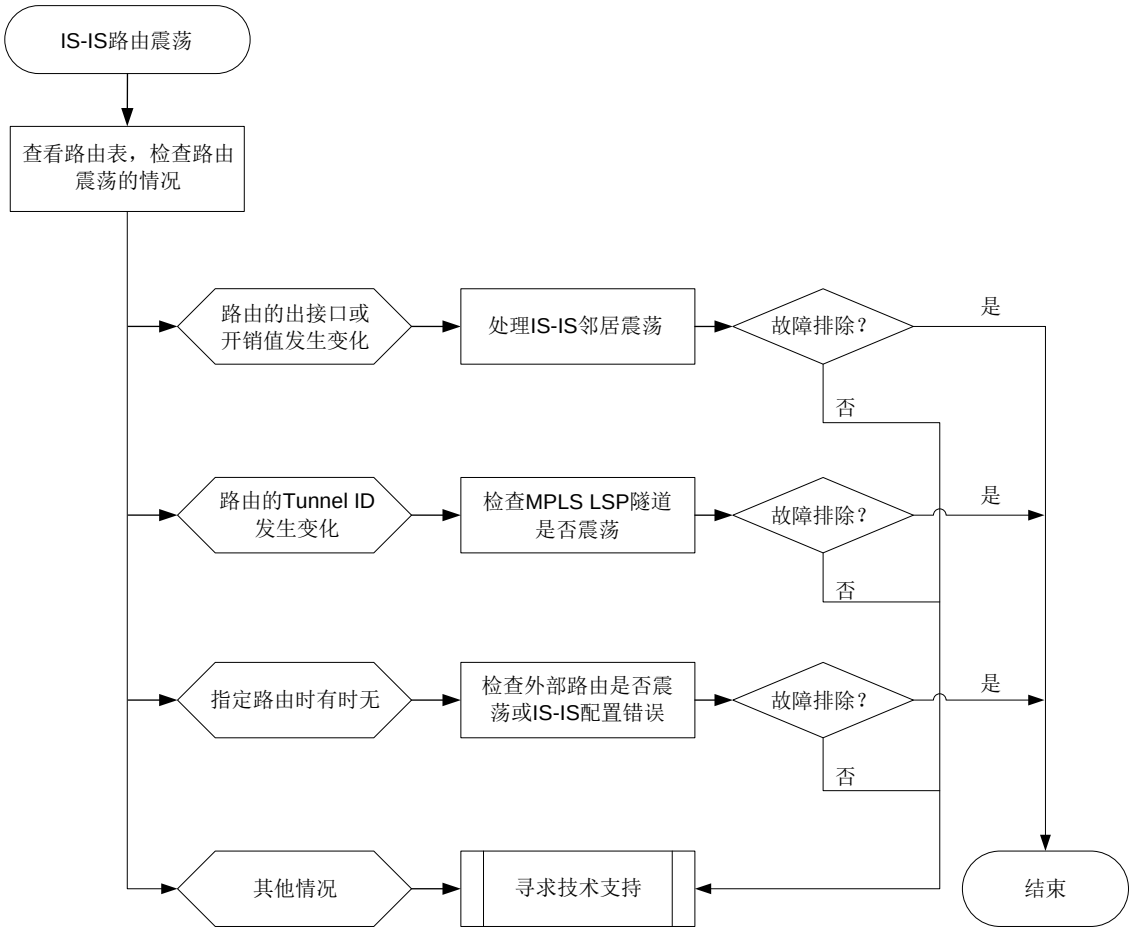
本类故障的常见原因主要包括：

- IS-IS 邻居震荡。
- MPLS LSP 隧道震荡。
- 两台设备的 IS-IS 引入了相同的外部路由，并且外部路由的优先级比 IS-IS 协议的优先级低。
- 两台设备配置的 System ID 相同。

3. 故障分析

本类故障的诊断流程如图 45 所示。

图45 IS-IS 路由震荡的故障诊断流程图



4. 处理步骤

(1) 检查路由震荡的情况。

执行 **display ip routing-table** *ip-address* **verbose** 命令，查看路由震荡的具体情况，具体步骤如下：

- 如果路由震荡的前后，“TunnelID”字段发生了变化，请检查 MPLS LSP 隧道是否存在震荡。

  执行 **display mpls lsp verbose** 命令，通过“Last Chg Time”字段查看 LDP 的 LSP 最近一次状态变化的时间。如果最近一次变化的时间距离执行 **display mpls lsp verbose** 命令的时间较近，说明 MPLS LSP 隧道存在震）。

  对于这种情况，请参考 LDP LSP 震荡的定位思路或 TE Tunnel 由 Up 突然变 Down 的定位思路，排查 LSP 震荡问题。

- 如果路由的“Cost”或者“Interface”字段发生变化，请检查该路由路径上的 IS-IS 邻居是否在震荡。

- 如果路由在路由表中时有时无（Age 字段在震荡），执行 **display isis lsdb verbose** 命令，找到携带该路由的 LSP，并记录此 LSP 报文的 LSPID。然后，执行 **display isis lsdb verbose lsp-id** 命令查看这条 LSP 的更新情况。

  – 如果 LSP 中一直携带指定的路由，请检查该路由路径上是否存在 IS-IS 邻居震荡。

- 如果 LSP 的“Seq Num”字段的取值在不停的增加，并且 LSP 更新前后的内容差异很大，请检查网络中是否有两台设备配置了相同的 System ID。
- 如果 LSP 的“Seq Num”字段的取值在不停的增加，并且 LSP 更新前后，指定的路由时有时无，请在产生该 LSP 的设备上执行步骤(2)。

  - 如果路由的“Protocol”字段发生变化，请执行步骤(2)。

(2) 检查 IS-IS 引入外部路由的配置。

如果指定的路由是作为外部路由引入到 IS-IS 的，在引入该路由的设备上，执行 **display ip routing-table** *ip-address* **verbose** 命令，查看路由震荡的具体情况，具体步骤如下：

- 如果路由表中处于“Active”状态的路由是 IS-IS 路由，而不是 IS-IS 引入的外部路由，说明网络中其他 IS-IS 设备发布了相同的路由。请根据网络规划修改路由协议的优先级，或者，在引入外部路由的 IS-IS 设备上配置路由过滤策略，控制下发到 IP 路由表的路由。
- 对于其它情况，请执行步骤(3)。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

9.3 OSPFv3故障处理

9.3.1 OSPFv3 邻居 Down

1. 故障描述

- OSPFv3 邻居 Down
- OSPFv3 邻居震荡

2. 常见原因

本类故障的常见原因主要包括：

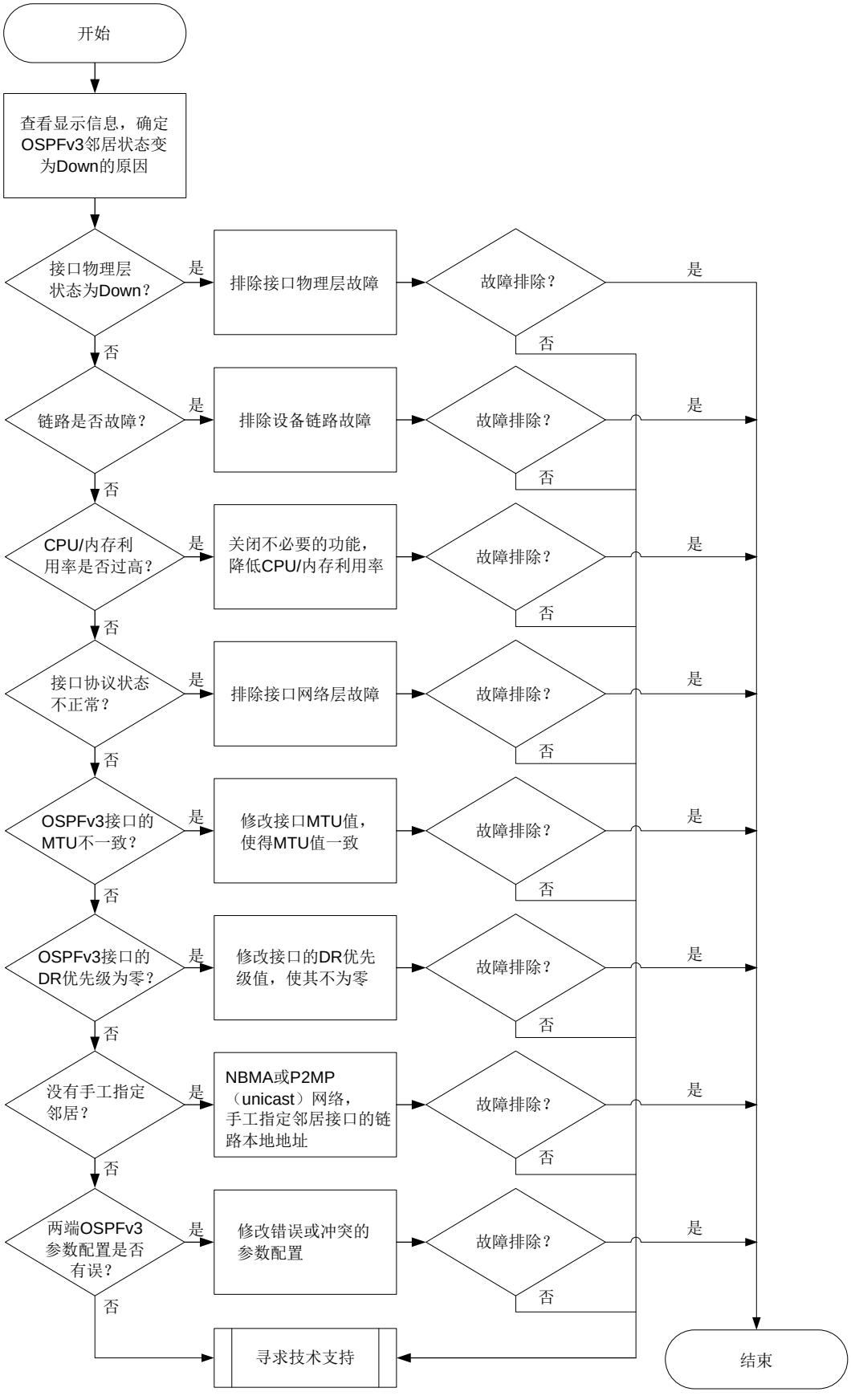
- BFD 会话 Down，即 BFD 检测到链路故障。
- 对端设备故障。
- CPU 利用率或内存利用率过高。
- 链路故障。
- OSPFv3 接口没有 Up。
- 两端 IP 地址不在同一网段。
- 两端 OSPFv3 参数的配置不匹配：
  - RouterID 配置冲突。
  - 两端区域类型配置不一致。

- 两端 OSPFv3 认证配置不匹配。
- 两端定时器参数配置不一致。
- OSPFv3 接口的网络类型不匹配。

3. 故障分析

本类故障的诊断流程如图 46 所示。

图46 OSPFv3 邻居 Down 的故障诊断流程图



4. 处理步骤

(1) 通过命令行查看 OSPFv3 邻居状态变为 Down 的原因。

执行 **display ospfv3 event-log peer** 命令，显示信息中的 Reason 字段为邻居状态发生变化的原因，一般包含如下几种情况：

- DeadExpired

  表示在邻居失效定时器超时前没有收到 Hello 报文，导致 OSPFv3 邻居状态变为 Down。出现这种情况请执行步骤(2)。

- BFDDown

  表示 BFD 会话 Down 导致 OSPFv3 邻居状态变为 Down。出现这种情况请执行步骤(2)。

- 1-Way

  表示对端 OSPFv3 状态首先变成 Down，然后向本端发送 1-way Hello 报文，导致本端 OSPFv3 状态变为 Init。出现这种情况请排查对端设备的故障。

- IntPhyChange

  表示接口 Down 或者接口 MTU 改变导致邻居关系变为 Down。此时，执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看接口的运行状态和相关信息，排查接口故障。其他情况请执行步骤 9.2.1 4. (11)。

(2) 检查接口的物理层状态是否为 Up。

执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看 OSPFv3 接口物理层状态，如果接口物理层状态为 Down 请先处理接口故障问题。如果接口物理状态为 Up，则执行步骤(3)。

(3) 检查链路是否故障。

请执行 **ping** 命令，检查设备链路是否故障（包括传输设备故障）。如果链路正常，请执行步骤(4)。

(4) 检查 CPU 利用率是否过高。

请执行 **display cpu-usage** 命令检查故障设备的主控板和接口板的 CPU 利用率是否过高。CPU 利用率过高会导致 OSPFv3 无法正常收发协议报文，继而导致邻居振荡。可通过关闭一些不必要的功能解决此问题。如果 CPU 利用率不高，则执行步骤(5)。

(5) 检查内存利用率是否超过了内存利用率阈值。

请执行 **display memory-threshold** 命令，查看显示信息中的 Current free-memory state，即系统当前内存使用状态。如果 Current free-memory state 为 Minor、Severe 或 Critical，表示剩余空闲内存较少，可能会导致设备无法收发 OSPFv3 报文或处理 OSPFv3 报文速度较慢，请关闭一些不必要的功能尝试解决此问题。如果系统当前内存使用状态为 Normal，则执行步骤(6)。

(6) 检查接口在 OSPFv3 协议下的状态是否正常。

执行 **display ospfv3 interface** 查看接口在 OSPFv3 协议下状态是否为正常状态。

- 如果 OSPFv3 接口状态为 Down，检查接口是否使能了 OSPFv3 功能。如果使能了 OSPFv3 功能，请处理网络层接口故障问题。

- 如果 OSPFv3 接口协议状态正常，即接口状态为 DR、BDR、DROther 或 P-2-P 时，请执行步骤(7)。

(7) 检查各 OSPFv3 接口的 MTU 是否一致。

如果接口下未配置 **ospfv3 mtu-ignore** 命令，则要求接口的 MTU 一致，否则无法建立 OSPFv3 邻居关系。请执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看接口 MTU 信息。

- 如果接口的 MTU 值配置不一致，请在接口视图下执行 **mtu** *size* 命令，将各个接口的 MTU 值修改为一致。
- 如果接口的 MTU 值一致，请执行步骤(8)。

(8) 检查各接口的 DR 优先级是否非零。

对于 Broadcast 和 NBMA 类型的网络，为了保证正确选举出 DR，需要保证至少有一个 OSPFv3 接口的 DR 优先级是非零的，否则两边的邻居状态只能达到 2-Way。请使用 **display ospfv3 interface** 命令查看 OSPFv3 接口信息，其中的 Priority 表示接口的 DR 优先级。

如果接口的 DR 优先级非零，请执行步骤(9)。

(9) 是否手工为 NBMA 网络或 P2MP 单播网络指定了邻居。

OSPFv3 网络类型为 NBMA 或 P2MP（unicast）时，必须通过 **ospfv3 peer** 命令手工指定邻居接口的链路本地地址。请在 OSPFv3 接口视图下使用 **display this** 命令查看接口的网络类型，如果接口的网络类型为 NBMA 或 P2MP（unicast），请在 OSPFv3 接口视图下使用 **ospfv3 peer** 命令手工指定邻居接口的链路本地地址。

如果手工为 NBMA 网络或 P2MP 单播网络指定了邻居接口的链路本地地址，请执行步骤(10)。

(10) 检查两端 OSPFv3 的参数配置是否有错误。

a. 请使用 **display ospfv3** 命令检查两端 OSPFv3 Router ID 配置是否冲突。如果 OSPFv3 Router ID 配置冲突，请修改配置保证 OSPFv3 Router ID 不再冲突。如果 OSPFv3 Router ID 配置不冲突，请继续执行以下检查。

b. 请使用 **display ospfv3 interface** 命令检查两端 OSPFv3 Area ID 配置是否一致。如果 OSPFv3 Area ID 配置不一致，请修改配置保证 OSPFv3 Area ID 配置一致。如果 OSPFv3 Area ID 配置一致，请继续执行以下检查。

c. 请使用 **display ospfv3 interface** 命令检查两端接口的 OSPFv3 网络类型是否一致。如果 OSPFv3 网络类型不一致，请修改配置保证 OSPFv3 网络类型一致。需要说明的是，如果双方一端为 PTP，另一端为 Broadcast，那么邻居关系可以达到 Full 状态，但无法计算出路由信息。

   如果接口的 OSPFv3 网络类型一致，请继续执行以下检查。

d. 请每隔 10 秒钟使用 **display ospfv3 statistics error** 命令检查一次 OSPFv3 的错误统计信息，并持续 5 分钟。需要查看的信息包括：

   - 查看 Authentication failure 字段。如果这个字段对应的计数值一直增长，表示建立邻居的两台设备配置的 OSPFv3 认证类型不一致，需要在两端设备上配置相同类型的认证。
   - 查看 HELLO: Hello-time mismatch 字段。如果这个字段对应的计数值一直在增长，表示接口上的 Hello 定时器的值不一致，需要将两端接口的 Hello 定时器的值设置为一致。
   - 查看 HELLO: Dead-time mismatch 字段。如果这个字段对应的计数值一直在增长，表示接口上的 Dead 定时器的值不一致，需要将两端接口的 Dead 定时器的值设置为一致。

– 查看 HELLO: Ebit option mismatch 字段。如果这个字段对应的计数值一直在增长，表示区域类型配置不一致（一端配置为普通区域，另一端配置为 Stub 或 NSSA 区域），需要将两端的区域类型设置为一致。

如果故障依然存在，请执行步骤(11)。

(11) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：OSPFV3-MIB

- ospfv3VirtIfStateChange (1.3.6.1.2.1.191.0.1)
- ospfv3NbrStateChange (1.3.6.1.2.1.191.0.2)
- ospfv3VirtNbrStateChange (1.3.6.1.2.1.191.0.3)

相关日志

- OSPFV3/6/OSPFV3_LAST_NBR_DOWN
- OSPFV3/5/OSPFV3_NBR_CHG

9.3.2 OSPFv3 邻居无法达到 FULL 状态

1. 故障描述

OSPFv3 的状态机包括 Down、Init、2-way、Exstart、Exchange、Loading 和 Full。其中，稳定状态包括 Down、2-way 和 Full：

- Down：表示未使能 OSPFv3。
- 2-way：DRother 之间的邻居关系。
- Full：形成邻接关系。

对于使用 OSPFv3 进行路由计算和路由转发的网络中，只有 2-way 和 Full 是正常的邻居状态。如果邻居状态既未处于 2-way 状态，也未处于 Full 状态，说明邻居关系不正常。

2. 常见原因

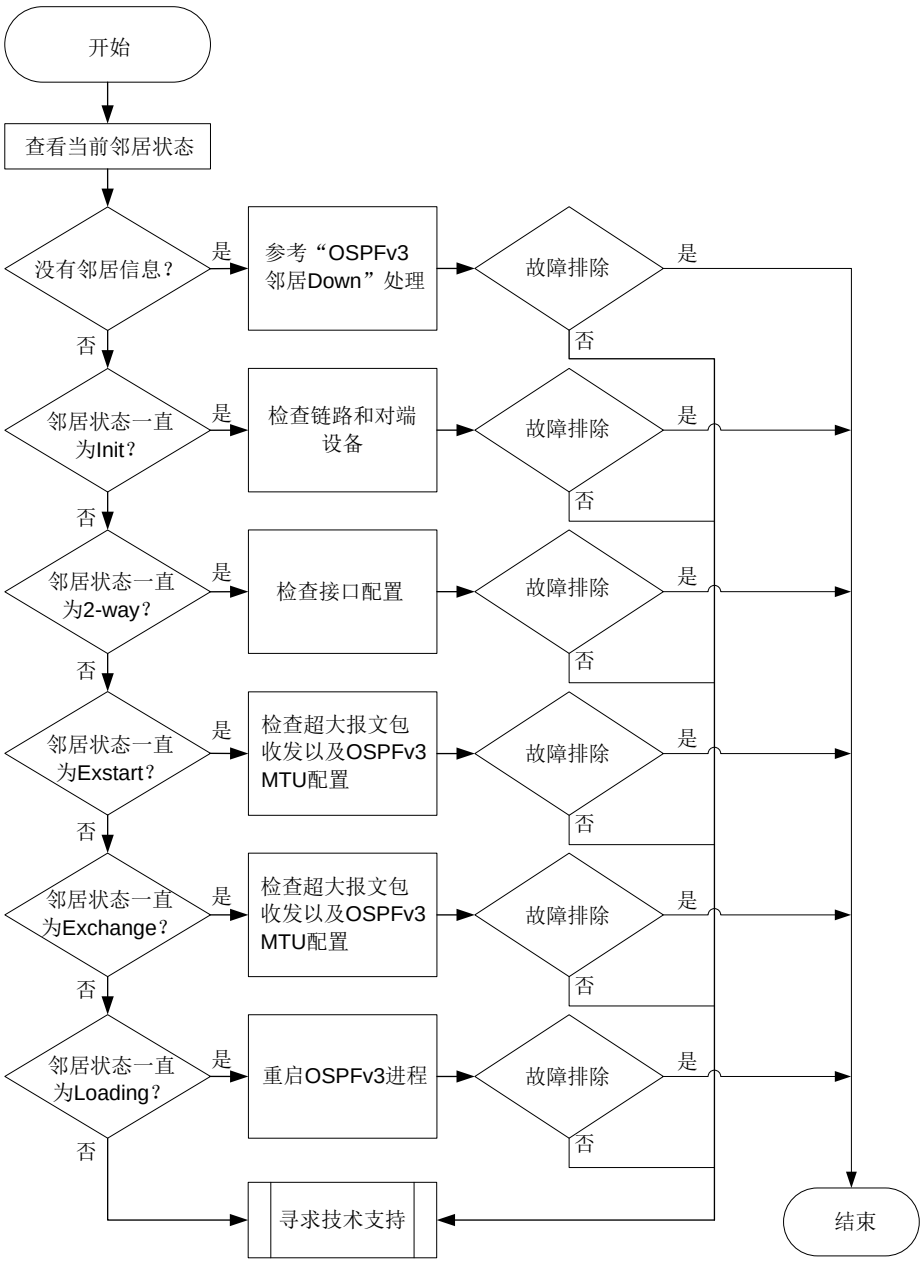
本类故障的常见原因主要包括：

- 链路故障，OSPFv3 报文被丢弃。
- 接口的 DR 优先级配置不合理。
- 两端配置的 OSPFv3 MTU 值不同。

3. 故障分析

本类故障的诊断流程如图 47 所示。

图47 OSPFv3 邻居 Down 的故障诊断流程图



4. 处理步骤

(1) 使用 **display ospfv3 peer** 命令查看 OSPFv3 邻居信息，并根据不同的邻居状态进行相应的处理。

- 没有邻居信息。

  请检查是否在 OSPFv3 进程下设置了 Router ID，如果未设置 Router ID，则 OSPFv3 进程无法运行。如果设置了 Router ID，则表示 OSPFv3 邻居 Down 或者邻居震荡，请参见“9.3.1 OSPFv3 邻居 Down”故障处理。

- 邻居状态一直为 Init。

  表示对端设备收不到本端发送的 Hello 报文，此时请排查链路和对端设备是否故障。

- 邻居状态一直为 2-way。

  执行命令 **display ospfv3 interface verbose** 命令查看设备在 OSPFv3 接口的 DR 优先级是否为 0：

  如果 OSPFv3 接口的 DR 优先级为 0，那么邻居状态为 2-way 属于正常情况。

  如果 OSPFv3 接口的 DR 优先级不为 0，请执行步骤 9.2.2 4. (2)。
- 邻居状态一直是 Exstart。

  表示设备一直在进行 DD 协商，但无法进行 DD 同步，出现该情况有两种可能性：

  – 接口无法正常收发超大报文

    可以通过多次执行命令 **ping -s** *packet-size neighbor-address* 查看超大报文收发情况，将 *packet-size* 设置为 1500 或更大数值。如果无法 Ping 通，请先解决链路问题。

  – 两端 OSPFv3 MTU 配置值不一致

    如果 OSPFv3 接口下配置了 **ospfv3 mtu-ignore** 命令，则无需检查两端的 OSPFv3 MTU 值是否相等；否则，需要检查两端的 OSPFv3 MTU 值是否相等，如果不相等则修改接口下的 MTU 值。

  如果故障没有解决，请执行步骤(2)。
- 邻居状态一直是 Exchange。

  表示设备在进行 DD 交换，请参见邻居状态一直为 Exstart 状态的处理。

  如果故障没有解决，请执行步骤(2)。
- 邻居状态一直是 Loading。

  如果使用 **display ospfv3 peer** 命令查看到邻居状态一直处于 Loading，可以尝试执行 **reset ospfv3** [*process-id*] **process** 命令重启 OSPFv3 进程。

  如果故障没有解决，请执行步骤(2)。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

9.4 OSPF故障处理

9.4.1 OSPF 邻居 Down

1. 故障描述

- OSPF 邻居 Down
- OSPF 邻居震荡

2. 常见原因

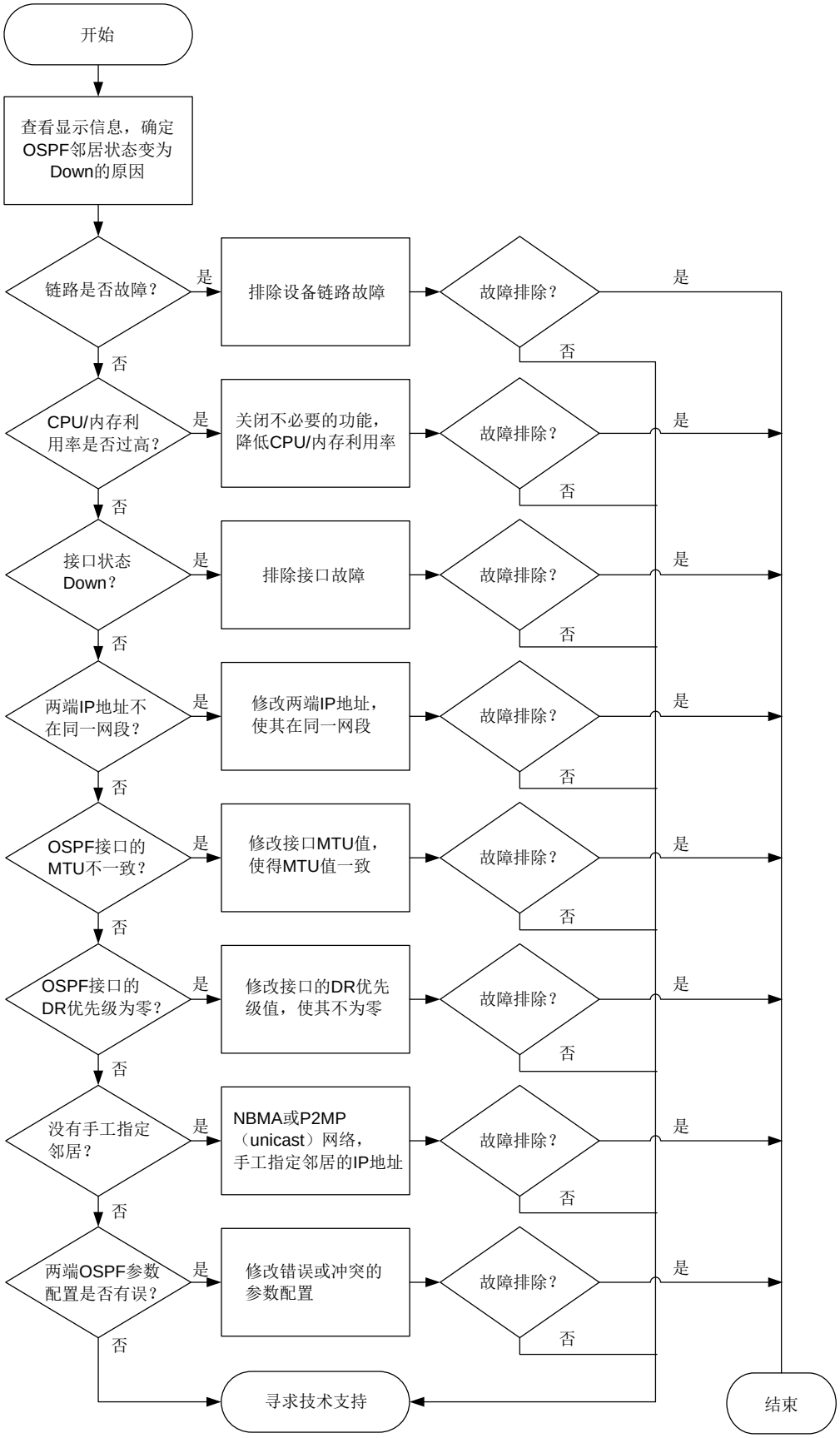
本类故障的常见原因主要包括：

- BFD 会话 Down，即 BFD 检测到链路故障。
- 对端设备故障。
- CPU 利用率过高。
- 链路故障。
- OSPF 接口没有 Up。
- 两端 IP 地址不在同一网段。
- OSPF 两端参数的配置不匹配：
  - Router ID 配置冲突。
  - 两端区域类型配置不一致。
  - 两端 OSPF 验证配置不匹配。
  - 两端定时器参数配置不一致。
  - OSPF 接口的网络类型不匹配。

3. 故障分析

本类故障的诊断流程如图 48 所示。

图48 OSPF 邻居 Down 的故障诊断流程图



4. 处理步骤

(1) 通过命令行或日志查看 OSPF 邻居状态变为 Down 的原因。

执行 **display ospf event-log peer** 命令，显示信息中的 Reason 字段为邻居状态发生变化的原因，一般包含如下几种情况：

- DeadExpired

  表示在邻居失效定时器超时前没有收到 Hello 报文，导致 OSPF 邻居状态变为 Down。出现这种情况请执行步骤 9.2.1 4. (1)。

- BFDDown

  表示 BFD 会话 Down 导致 OSPF 邻居状态变为 Down。出现这种情况请执行步骤 9.2.1 4. (1)。

- IntVliChange 或 virtual link was deleted or the route it relies on was deleted

  表示虚连接删除或者其依赖的路由删除导致邻居关系变为 Down。出现这种情况请执行步骤 9.2.1 4. (1)。

- 1-Way

  表示对端 OSPF 状态首先变成 Down，然后向本端发送 1-way Hello 报文，导致本端 OSPF 状态变为 Init。出现这种情况请排查对端设备的故障。

- IntPhyChange

  接口 Down 或者接口 MTU 改变导致邻居关系变为 Down。此时，执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]] 命令查看接口的运行状态和相关信息，排查接口故障。其他情况请执行步骤 9.2.1 4. (11)。

(2) 检查链路是否故障。

请执行 **ping** 命令，检查设备链路是否故障（包括传输设备故障）。如果链路正常，请执行步骤(3)。

(3) 检查 CPU 利用率是否过高。

请执行 **display cpu-usage** 命令检查故障设备的主控板和接口板的 CPU 利用率是否过高。CPU 利用率过高会导致 OSPF 无法正常收发协议报文从而导致邻居振荡。可通过关闭一些不必要的功能解决此问题。如果 CPU 利用率不高，则执行步骤(4)。

(4) 检查内存利用率是否超过了内存利用率阈值。

请执行 **display memory-threshold** 命令，查看显示信息中的 Current free-memory state，即系统当前内存使用状态。如果 Current free-memory state 为 Minor、Severe 或 Critical，表示剩余空闲内存较少，可能会导致设备无法收发 OSPF 报文或处理 OSPF 报文速度较慢，请关闭一些不必要的功能尝试解决此问题。如果系统当前内存使用状态为 Normal，则执行步骤(5)。

(5) 检查接口状态是否为 Up。

执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看接口物理层状态，如果接口物理层状态为 Down 请先处理接口故障问题。如果接口物理层状态是 Up，请执行 **display ospf interface** 查看接口在 OSPF 协议下状态是否为正常状态：

- 如果 OSPF 接口状态为 Down，检查 OSPF 进程下是否通过 **network** 命令通告了接口所属网段。如果 OSPF 未通告接口所属网段，则检查接口下是否使能了 OSPF。如果接口使能了 OSPF 进程，请处理网络层接口故障问题。
- 如果 OSPF 下的接口协议状态正常，即接口状态为 DR、BDR、DROther 或 PTP 时，请执行步骤(6)。

(6) 检查两端 IP 地址是否在同一网段。

请执行 **display interface brief** 命令查看两端接口的 IP 地址：

- 如果两端接口的 IP 地址不在同一网段，请在接口视图下执行 **ip address** 命令修改两端的 IP 地址，使其在同一网段。
- 如果两端接口的 IP 地址处于同一网段，请执行步骤(7)。

(7) 检查各 OSPF 接口的 MTU 是否一致。

如果在 OSPF 接口上通过 **ospf mtu-enable** 命令将该接口发送的 DD 报文中 MTU 域的值填充为接口的 MTU 值（缺省情况下接口发送的 DD 报文中 MTU 域的值为 0），则要求各个 OSPF 接口发送的 DD 报文中 MTU 域的值一致。否则，OSPF 邻居无法协商成功。请执行 **display interface** [*interface-type* [*interface-number* | *interface-number.subnumber*]]命令查看接口 MTU 信息：

- 如果接口的 MTU 值配置不一致，请在接口视图下执行 **mtu** *size* 命令，将各个接口的 MTU 值修改为一致。
- 如果接口的 MTU 值一致，请执行步骤(8)。

(8) 检查各接口的 DR 优先级是否非零。

对于 Broadcast 和 NBMA 类型的网络，为了保证正确选举出 DR，需要保证至少有一个 OSPF 接口的 DR 优先级是非零的，否则两边的邻居状态只能达到 2-Way。请使用 **display ospf interface** 命令查看 OSPF 接口信息，其中的 Pri 表示接口的 DR 优先级。

如果接口的 DR 优先级非零，请执行步骤(9)。

(9) 是否手工为 NBMA 网络或 P2MP 单播网络指定了邻居。

OSPF 网络类型为 NBMA 或 P2MP（unicast）时，必须通过 **peer** 命令手工指定邻居的 IP 地址。请在 OSPF 接口视图下使用 **display this** 命令查看接口的网络类型，如果接口的网络类型为 NBMA 或 P2MP（unicast），请在 OSPF 视图下使用 **peer** 命令手工指定邻居的 IP 地址。

如果手工为 NBMA 网络或 P2MP 单播网络指定了邻居的 IP 地址，请执行步骤(10)。

(10) 检查两端 OSPF 的参数配置是否有错误。

a. 请使用 **display ospf** 命令检查两端 OSPF Router ID 配置是否冲突。如果 OSPF Router ID 配置冲突，请修改配置保证 OSPF Router ID 不再冲突。如果 OSPF Router ID 配置不冲突，请继续执行以下检查。

b. 请使用 **display ospf interface** 命令检查两端 OSPF Area ID 配置是否一致。如果 OSPF Area ID 配置不一致，请修改配置保证 OSPF Area ID 配置一致。如果 OSPF Area ID 配置一致，请继续执行以下检查。

c. 请使用 **display ospf interface** 命令检查两端接口的 OSPF 网络类型是否一致。如果 OSPF 网络类型不一致，请修改配置保证 OSPF 网络类型一致。需要说明的是，如果双方一端为 PTP，另一端为 Broadcast，那么邻居关系可以达到 Full 状态，但无法计算出路由信息。

如果接口的 OSPF 网络类型一致，请继续执行以下检查。

d. 请每隔 10 秒钟使用 **display ospf statistics error** 命令检查一次 OSPF 的错误统计信息，并持续 5 分钟。需要查看的信息包括：

- 查看 Bad authentication type 字段。如果这个字段对应的计数值一直增长，表示建立邻居的两台设备配置的 OSPF 认证类型不一致，需要在两端设备上配置相同认证的类型。
- 查看 Hello-time mismatch 字段。如果这个字段对应的计数值一直在增长，表示接口上的 Hello 定时器的值不一致，需要将两端接口的 Hello 定时器的值设置为一致。
- 查看 Dead-time mismatch 字段。如果这个字段对应的计数值一直在增长，表示接口上的 Dead 定时器的值不一致，需要将两端接口的 Dead 定时器的值设置为一致。
- 查看 Ebit option mismatch 字段。如果这个字段对应的计数值一直在增长，表示区域类型配置不一致（一端配置为普通区域，另一端配置为 Stub 或 NSSA 区域），需要将两端的区域类型设置为一致。

如果故障依然存在，请执行步骤(11)。

(11) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：OSPF-TRAP-MIB

- ospfVirtIfStateChange (1.3.6.1.2.1.14.16.2.1)
- ospfNbrStateChange (1.3.6.1.2.1.14.16.2.2)
- ospfVirtNbrStateChange (1.3.6.1.2.1.14.16.2.3)

相关日志

- OSPF/5/OSPF_NBR_CHG
- OSPF/5/OSPF_NBR_CHG_REASON

9.4.2 OSPF 邻居无法达到 FULL 状态

1. 故障描述

OSPF 的状态机包括 Down、Init、2-way、Exstart、Exchange、Loading 和 Full。其中，稳定状态包括 Down、2-way 和 Full：

- Down：表示未使能 OSPF。
- 2-way：DRother 之间的邻居关系。
- Full：形成邻接关系。

对于使用 OSPF 进行路由计算和路由转发的网络中，只有 2-way 和 Full 是正常的邻居状态。如果邻居状态既未处于 2-way 状态、也未处于 Full 状态，说明邻居关系不正常。

2. 常见原因

本类故障的常见原因主要包括：

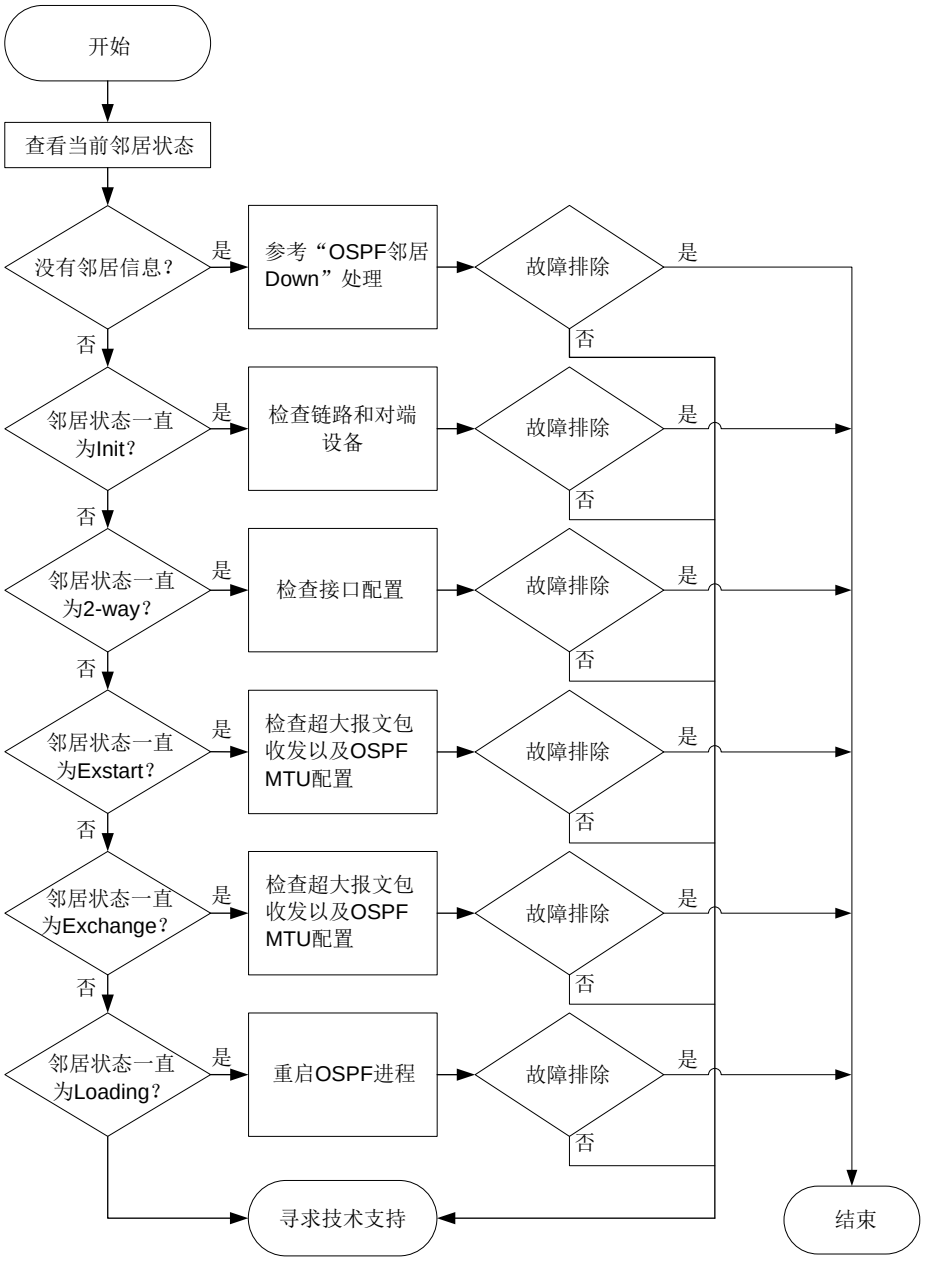
- 链路故障，OSPF 报文被丢弃。

- 接口的 DR 优先级配置不合理。
- 两端配置的 OSPF MTU 值不同。

3. 故障分析

本类故障的诊断流程如图 49 所示：

图49 OSPF 邻居无法达到 FULL 状态的故障诊断流程图



4. 处理步骤

(1) 使用 **`display ospf peer`** 命令查看 OSPF 邻居信息，并根据不同的邻居状态进行相应的处理。

- 没有邻居信息。

表示 OSPF 邻居 Down 或者邻居震荡，请参见“9.4.1 OSPF 邻居 Down”故障处理。

- 邻居状态一直为 Init。

  表示对端设备收不到本端发送的 Hello 报文，此时请排查链路和对端设备是否故障。

- 邻居状态一直为 2-way。

  执行命令 **display ospf interface verbose** 查看设备在 OSPF 接口的 DR 优先级是否为 0：

  - 如果 OSPF 接口的 DR 优先级为 0，那么邻居状态为 2-way 属于正常情况。
  - 如果 OSPF 接口的 DR 优先级不为 0，请执行步骤 9.2.2 4. (2)。

- 邻居状态一直是 Exstart。

  表示设备一直在进行 DD 协商，但无法进行 DD 同步，出现该情况有两种可能性：

  - 接口无法正常收发超大报文。

    可以通过多次执行命令 **ping -s** *packet-size neighbor-address* 查看超大报文收发情况，将 *packet-size* 设置为 1500 或更大数值。如果无法 Ping 通，请先解决链路问题。

  - 两端 OSPF MTU 配置值不一致。

    如果 OSPF 接口下配置了 **ospf mtu-enable** 命令，请检查两端的 OSPF MTU 值是否相等。如果不相等，则修改接口下的 MTU 值。

  如果故障没有解决，请执行步骤(2)。

- 邻居状态一直是 Exchange。

  表示设备在进行 DD 交换，请参见邻居状态一直为 Exstart 状态的处理。

  如果故障没有解决，请执行步骤(2)。

- 邻居状态一直是 Loading。

  如果使用 **display ospf peer** 命令查看邻居状态一直处于 Loading，可以尝试执行 **reset ospf** [*process-id*] **process** 命令重启 OSPF 进程。

  如果故障没有解决，请执行步骤(2)。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

9.4.3 设备学习不到部分 OSPF 路由

1. 故障描述

运行 OSPF 的设备学习不到部分 OSPF 路由。

2. 常见原因

本类故障的常见原因主要包括：

- 双方一端的网络类型为 P2P，另一端的网络类型为 Broadcast，邻居关系达到 Full 状态，但是学习不到路由。
- OSPF 进程下配置了 **filter-policy import** 命令。
- 本 OSPF 区域下配置了 **filter import** 命令。
- 其他 OSPF 区域下配置了 **filter export** 命令。
- 绑定了 VPN 实例的 OSPF 进程，该进程引入外部路由的 Tag 值与 AS External LSA（Type-5）或 NSSA External LSA（Type-7）中的 Tag 值一致。
- ABR 设备不可达。
- 在 ABR 设备上，非骨干区的 Summary LSA 不参与路由计算。
- ASBR 设备不可达。
- AS External LSA（Type-5）或 NSSA External LSA（Type-7）的 FA 地址不可达。
- NSSA External LSA（Type-7）到达 FA 地址的路由与 NSSA External LSA（Type-7）不在同一区域。

3. 故障分析

本类故障的诊断流程如图 50、图 51 所示。

图50 设备学习不到 OSPF 路由故障诊断流程图一

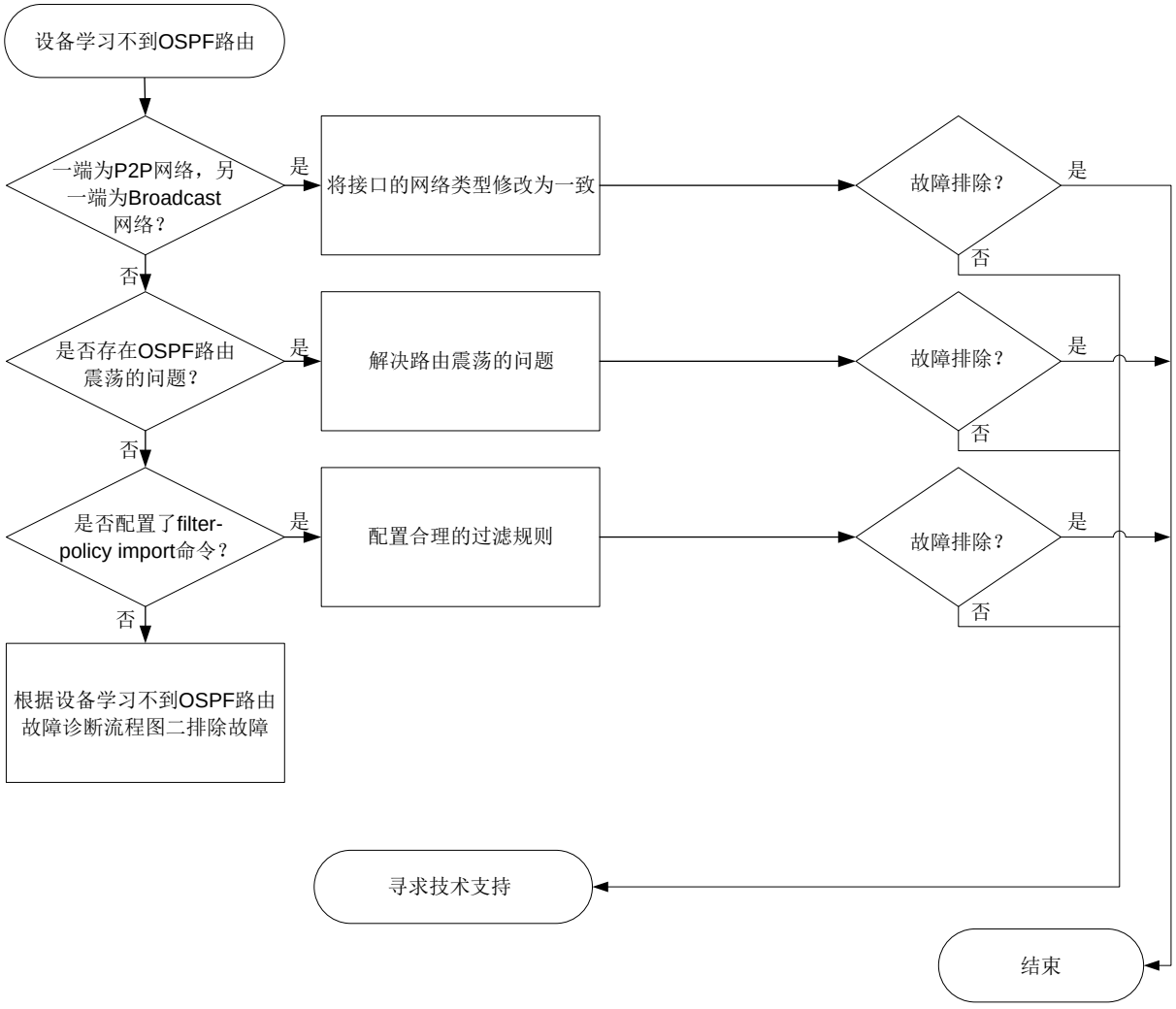
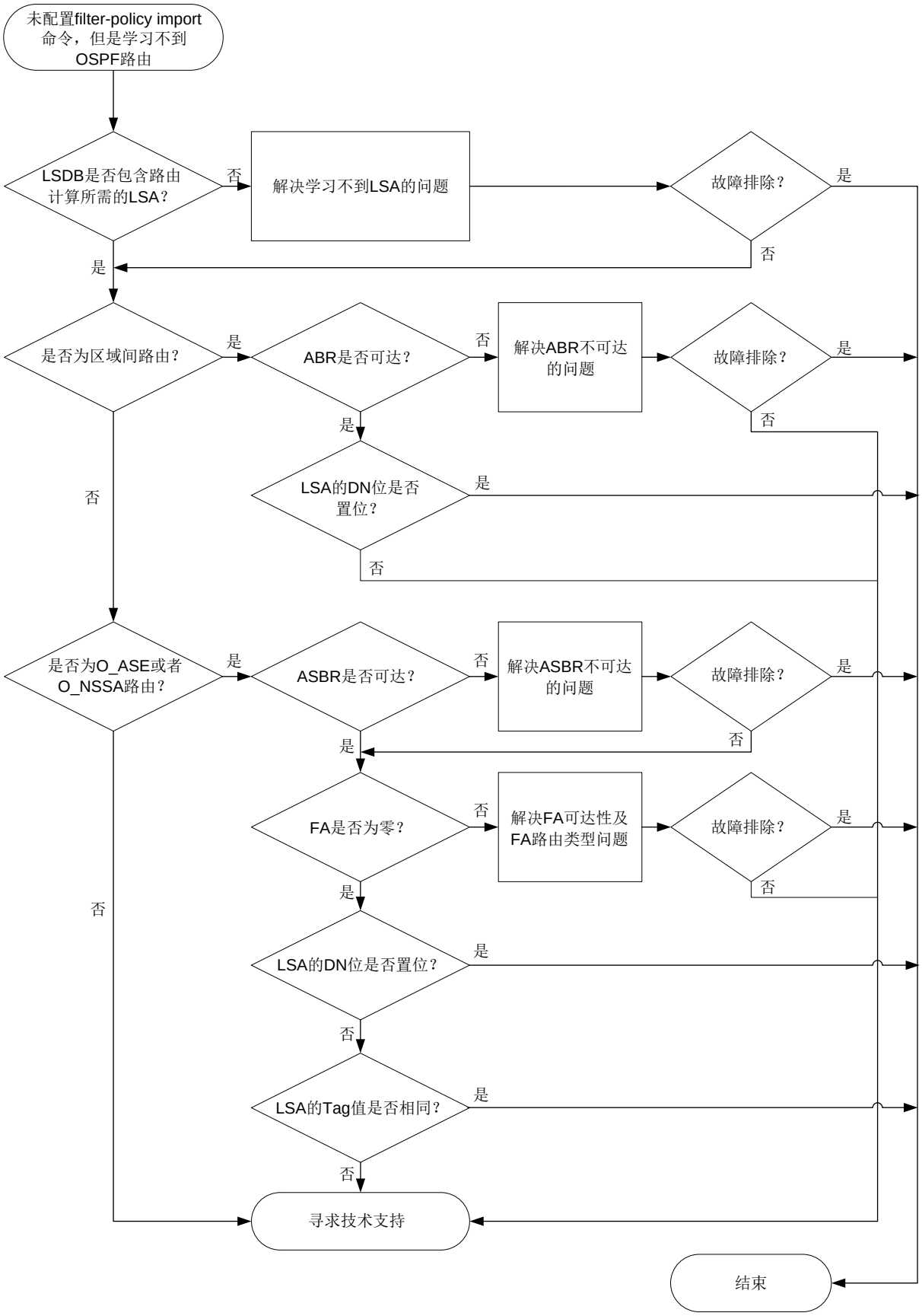


图51 设备学习不到 OSPF 路由故障诊断流程图二



4. 处理步骤

(1) 检查建立邻居关系的双方是否一端的网络类型为 P2P，另一端的网络类型为 Broadcast。

如果一端的网络类型为 P2P，另一端的网络类型为 Broadcast，那么邻居关系可以达到 Full 状态，但无法计算出路由信息。

a. 请执行 **display ospf interface** 命令查看接口的网络类型。

```
<Sysname> display ospf interface
         OSPF Process 1 with Router ID 5.5.5.5
                 Interfaces
 Area: 0.0.0.1
 IP Address      Type      State    Cost  Pri   DR              BDR
 192.168.51.5    PTP       P-2-P    1     1     0.0.0.0         0.0.0.0
```

b. 如果存在上述情况，请在 OSPF 接口视图下执行 **ospf network-type** 命令将本端设备与邻居设备的 OSPF 接口网络类型配置为一致。

如果不存在上述情况，请执行步骤(2)。

(2) 多次查看 OSPF 路由表，检查是否存在 OSPF 路由震荡的问题。

请执行 **display ip routing-table protocol ospf verbose** 命令，查看 Age 字段，确认是否存在震荡的 OSPF 路由。

- 如果某条或某些 OSPF 路由 Age 字段的数值一直很小，说明相应的 OSPF 路由发生震荡，请解决路由震荡问题。
- 如果不存在路由震荡的问题，请执行步骤(3)。

```
<Sysname> display ip routing-table protocol ospf verbose

Summary count : 3

 Destination: 192.168.12.0/24
    Protocol: O_INTER
  Process ID: 1
   SubProtID: 0x2                    Age: 12h53m09s
        Cost: 2                Preference: 10
       IpPre: N/A              QosLocalID: N/A
         Tag: 0                    State: Active Adv
   OrigTblID: 0x0                OrigVrf: default-vrf
     TableID: 0x2                 OrigAs: 0
       NibID: 0x13000003          LastAs: 0
      AttrID: 0xffffffff        Neighbor: 0.0.0.0
       Flags: 0x10041         OrigNextHop: 192.168.51.1
       Label: NULL            RealNextHop: 192.168.51.1
     BkLabel: NULL              BkNextHop: N/A
     SRLabel: NULL              Interface: GigabitEthernet1/0/2
   BkSRLabel: NULL            BkInterface: N/A
    SIDIndex: NULL                InLabel: NULL
   Tunnel ID: Invalid         IPInterface: GigabitEthernet1/0/2
 BkTunnel ID: Invalid       BkIPInterface: N/A
    FtnIndex: 0x0           ColorInterface: N/A
```

```
TrafficIndex: N/A          BkColorInterface: N/A
   Connector: 0.0.0.0             VpnPeerId: N/A
        Dscp: N/A                     Exp: N/A
  SRTunnelID: Invalid             StatFlags: 0x0
    SID Type: N/A                     SID: N/A
       BkSID: N/A                     NID: Invalid
    FlushNID: Invalid                BkNID: Invalid
  BkFlushNID: Invalid               PathID: 0x0
CommBlockLen: 0
  OrigLinkID: 0x0                RealLinkID: 0x0

 Destination: 192.168.24.0/24
    Protocol: O_INTER
  Process ID: 1
   SubProtID: 0x2                       Age: 12h53m09s
        Cost: 3                  Preference: 10
       IpPre: N/A                QosLocalID: N/A
         Tag: 0                       State: Active Adv
   OrigTblID: 0x0                   OrigVrf: default-vrf
     TableID: 0x2                    OrigAs: 0
       NibID: 0x13000003             LastAs: 0
      AttrID: 0xffffffff           Neighbor: 0.0.0.0
       Flags: 0x10041           OrigNextHop: 192.168.51.1
       Label: NULL              RealNextHop: 192.168.51.1
     BkLabel: NULL                BkNextHop: N/A
     SRLabel: NULL                Interface: GigabitEthernet1/0/2
   BkSRLabel: NULL              BkInterface: N/A
    SIDIndex: NULL                  InLabel: NULL
   Tunnel ID: Invalid           IPInterface: GigabitEthernet1/0/2
 BkTunnel ID: Invalid         BkIPInterface: N/A
    FtnIndex: 0x0              ColorInterface: N/A
TrafficIndex: N/A          BkColorInterface: N/A
   Connector: 0.0.0.0             VpnPeerId: N/A
        Dscp: N/A                     Exp: N/A
  SRTunnelID: Invalid             StatFlags: 0x0
    SID Type: N/A                     SID: N/A
       BkSID: N/A                     NID: Invalid
    FlushNID: Invalid                BkNID: Invalid
  BkFlushNID: Invalid               PathID: 0x0
CommBlockLen: 0
  OrigLinkID: 0x0                RealLinkID: 0x0

 Destination: 192.168.51.0/24
    Protocol: O_INTRA
  Process ID: 1
   SubProtID: 0x1                       Age: 12h54m07s
        Cost: 1                  Preference: 10
       IpPre: N/A                QosLocalID: N/A
```

```
          Tag: 0                       State: Inactive Adv
   OrigTblID: 0x0                   OrigVrf: default-vrf
     TableID: 0x2                    OrigAs: 0
       NibID: 0x13000001             LastAs: 0
      AttrID: 0xffffffff           Neighbor: 0.0.0.0
       Flags: 0x10c1            OrigNextHop: 0.0.0.0
       Label: NULL              RealNextHop: 0.0.0.0
     BkLabel: NULL                BkNextHop: N/A
     SRLabel: NULL                Interface: GigabitEthernet1/0/2
   BkSRLabel: NULL              BkInterface: N/A
    SIDIndex: NULL                  InLabel: NULL
   Tunnel ID: Invalid           IPInterface: GigabitEthernet1/0/2
 BkTunnel ID: Invalid         BkIPInterface: N/A
    FtnIndex: 0x0             ColorInterface: N/A
TrafficIndex: N/A          BkColorInterface: N/A
   Connector: 0.0.0.0              VpnPeerId: N/A
        Dscp: N/A                        Exp: N/A
  SRTunnelID: Invalid              StatFlags: 0x0
    SID Type: N/A                        SID: N/A
       BkSID: N/A                        NID: Invalid
    FlushNID: Invalid                 BkNID: Invalid
  BkFlushNID: Invalid                PathID: 0x0
CommBlockLen: 0
  OrigLinkID: 0x0                 RealLinkID: 0x0
```

(3) 检查 OSPF 进程下是否配置了 **filter-policy import** 命令。

某些场景下需要对路由信息进行过滤，实现业务隔离。请检查是否存在 OSPF 路由被错误过滤的情况。

a. 请在本端设备出现问题的 OSPF 进程下执行 **display this** 命令，查看该 OSPF 进程下是否配置了 **filter-policy import** 命令，导致 OSPF 路由被过滤。

```
[Sysname-ospf-1] display this
#
ospf 1
 import-route direct
 filter-policy 2000 import
 area 0.0.0.1
  network 192.168.51.0 0.0.0.255
  nssa
#
return
```

b. 如果 OSPF 进程下配置了 **filter-policy import** 命令，请查看该命令引用的过滤规则的配置信息。

- 对于 **filter-policy import** 命令引用 ACL 规则进行路由过滤的情况，请执行 **display acl** { *acl-number* | **name** *acl-name* }命令查看 ACL 的配置信息。
- 对于 **filter-policy import** 命令引用前缀列表进行路由过滤的情况，请执行 **display ip prefix-list** 命令查看地址前缀列表的配置信息。

– 对于 **filter-policy import** 命令引用路由策略进行路由过滤的情况，请执行 **display route-policy** 命令查看路由策略的配置信息。

如果路由被过滤规则拒绝，请结合组网及实际业务需求确认过滤规则的配置是否合理。如果不合理，请修改 **filter-policy import** 命令引用的过滤规则。

c. 如果该路由没有被拒绝，或者该 OSPF 进程并没有配置 **filter-policy import** 过滤策略，请执行步骤(4)。

(4) 检查 OSPF 进程的 LSDB 是否包含未学习到的 OSPF 路由的 LSA。

请根据 OSPF 进程未学习到的路由信息的类型选择不同的故障处理方式。

o OSPF 区域内路由

如果 OSPF 进程缺失区域内路由，请在用户视图下执行 **display ospf** [*process-id*] **lsdb router** 命令，检查 LSDB 是否包含该区域中所有的 Router LSA 信息。

```
<Sysname> display ospf 100 lsdb router

         OSPF Process 100 with Router ID 5.5.5.5
                     Area: 0.0.0.1
             Link State Database


    Type      : Router
    LS ID     : 5.5.5.5
    Adv Rtr   : 5.5.5.5
    LS age    : 7
    Len       : 36
    Options   : ASBR O NP
    Seq#      : 80000026
    Checksum  : 0x5f1f
    Link Count: 1
       Link ID: 192.168.51.1
       Data   : 192.168.51.5
       Link Type: TransNet
       Metric : 1

    Type      : Router
    LS ID     : 1.1.1.1
    Adv Rtr   : 1.1.1.1
    LS age    : 8
    Len       : 36
    Options   : ASBR ABR O NP
    Seq#      : 8000002a
    Checksum  : 0x534a
    Link Count: 1
       Link ID: 192.168.51.1
       Data   : 192.168.51.1
       Link Type: TransNet
       Metric : 1
```

– 如果 OSPF 进程的 LSDB 缺失 Router LSA，请执行步骤(7)。

– 如果 OSPF 进程的 LSDB 包含完整的 Router LSA，但是无法计算出路由信息，请执行步骤(7)。

o OSPF 区域间路由

如果 OSPF 进程缺失区域间路由，请在用户视图下执行 **display ospf** [*process-id*] **lsdb summary** 命令，检查 LSDB 是否包含其他所有区域的 Network Summary LSA。

```
<Sysname> display ospf lsdb summary

         OSPF Process 1 with Router ID 5.5.5.5
                     Area: 0.0.0.1
             Link State Database


    Type      : Sum-Net
    LS ID     : 192.168.24.0
    Adv Rtr   : 1.1.1.1
    LS age    : 576
    Len       : 28
    Options   : O NP
    Seq#      : 8000001f
    Checksum  : 0x4c25
    Net Mask  : 255.255.255.0
    Tos 0  Metric: 2

    Type      : Sum-Net
    LS ID     : 192.168.12.0
    Adv Rtr   : 1.1.1.1
    LS age    : 576
    Len       : 28
    Options   : O NP
    Seq#      : 8000001f
    Checksum  : 0xc6b7
    Net Mask  : 255.255.255.0
    Tos 0  Metric: 1
```

– 如果 OSPF 进程的 LSDB 缺失 Network Summary LSA，检查本区域下是否配置了 **filter import** 命令，或者 Network Summary LSA 的发布者所在区域下是否配置了 **filter export** 命令。如果 **filter import** 命令或 **filter export** 命令引用的过滤规则错误地过滤掉了 Network Summary LSA，请修改过滤规则相关配置。

filter import 命令和 **filter export** 命令可以引用 ACL、前缀列表、路由策略对 Network Summary LSA 进行过滤，请分别使用 **display acl** { *acl-number* | **name** *acl-name* }命令、**display ip prefix-list** 命令、**display route-policy** 命令查看相应的配置信息。

– 如果 OSPF 进程的 LSDB 包含完整的 Network Summary LSA，但是无法计算出路由信息，请执行步骤(7)。

o O_ASE 路由或者 O_NSSA 路由

如果 OSPF 进程缺失 O_ASE 路由，请在用户视图下执行 **display ospf** [*process-id*] **lsdb ase** 命令。检查 LSDB 是否包含 AS External LSA。

```
<Sysname> display ospf 100 lsdb ase

         OSPF Process 100 with Router ID 1.1.1.1
                 Link State Database


    Type      : External
    LS ID     : 10.1.1.0
    Adv Rtr   : 1.1.1.1
    LS age    : 713
    Len       : 36
    Options   : O E
    Seq#      : 80000001
    Checksum  : 0x934b
    Net Mask  : 255.255.255.0
    TOS 0  Metric: 1
    E Type    : 2
    Forwarding Address : 192.168.51.5
    Tag       : 1
```

如果 OSPF 进程缺失 O_NSSA 路由，请在用户视图下执行 **display ospf** [*process-id*] **lsdb nssa** 命令，检查 LSDB 是否包含 NSSA External LSA。

```
<Sysname> display ospf 100 lsdb nssa

         OSPF Process 100 with Router ID 1.1.1.1
                        Area: 0.0.0.0
                 Link State Database

                        Area: 0.0.0.1
                 Link State Database


    Type      : NSSA
    LS ID     : 192.168.51.0
    Adv Rtr   : 5.5.5.5
    LS age    : 965
    Len       : 36
    Options   : O NP
    Seq#      : 8000001f
    Checksum  : 0x1dfa
    Net Mask  : 255.255.255.0
    TOS 0  Metric: 1
    E Type    : 2
    Forwarding Address : 192.168.51.5
    Tag       : 1

    Type      : NSSA
    LS ID     : 10.1.1.0
    Adv Rtr   : 5.5.5.5
```

```
LS age    : 965
Len       : 36
Options   : O NP
Seq#      : 8000001f
Checksum  : 0x6840
Net Mask  : 255.255.255.0
TOS 0  Metric: 1
E Type    : 2
Forwarding Address : 192.168.51.5
Tag       : 1
```

- 如果 OSPF 进程的 LSDB 缺失 AS External LSA 或 NSSA External LSA，请执行步骤(7)。
- 如果 OSPF 进程的 LSDB 包含完整的 AS External LSA 或 NSSA External LSA，但是无法学习到 O_ASE 路由或者 O_NSSA 路由的情况，请执行步骤(7)。

(5) 检查 ABR 设备是否可达。

区域间路由是 ABR 设备发布的，如果本端设备和 ABR 设备之间路由不可达，则会导致本端设备无法学习到区域间路由。

a. 请在本端设备执行 **display ospf** [*process-id*] **lsdb summary** 命令，查看 Adv Rtr 字段，该字段为通告 Network Summary LSA 的 Router ID，即 ABR 的 Router ID。

```
<Sysname> display ospf 100 lsdb summary

         OSPF Process 100 with Router ID 5.5.5.5
                     Area: 0.0.0.1
             Link State Database



Type      : Sum-Net
LS ID     : 192.168.12.0
Adv Rtr   : 1.1.1.1
LS age    : 913
Len       : 28
Options   : O E
Seq#      : 80000001
Checksum  : 0x5d45
Net Mask  : 255.255.255.0
Tos 0  Metric: 1
```

b. 请在本端设备执行 **display ospf abr-asbr** 命令，查看 Destination 字段和 RtType 字段，RtType 字段取值为 ABR 时，Destination 字段为 ABR 的 Router ID。查看到此类路由信息时，说明存在到达为 ABR 的路由。

```
<Sysname> display ospf 100 abr-asbr

         OSPF Process 100 with Router ID 5.5.5.5
                 Routing Table to ABR and ASBR

 Type    Destination     Area            Cost     Nexthop         RtType
 Intra   1.1.1.1         0.0.0.1         1        192.168.51.1    ABR
```

c. 如果 abr-asbr 信息中不包含到达通告 Network Summary LSA 的 ABR 的路由，请执行步骤(7)。

d. 如果 abr-asbr 信息中包含到达通告 Network Summary LSA 的 ABR 的路由，且本设备为 ABR 设备，请检查 OSPF 区域是否为骨干区域。

   – 如果 OSPF 区域为非骨干区域（区域 ID 不为零），根据 RFC 2328 的规定，ABR 设备不会对非骨干区的 Network Summary LSA 进行计算，没有区域间路由是正常现象。

   – 如果 OSPF 区域为骨干区域（区域 ID 为零），但是没有学习到区域间路由，请执行步骤(7)。

e. 如果 abr-asbr 信息中包含到达通告 Network Summary LSA 的 ABR 的路由，且本 OSPF 进程绑定了 VPN 实例。请检查 OSPF 进程下是否配置了 **vpn-instance-capability simple** 命令。如果 OSPF 进程下配置了 **vpn-instance-capability simple** 命令，请执行步骤(7)。

   如果 OSPF 进程下未配置 **vpn-instance-capability simple** 命令，故障处理方式如表 5 所示。

   表5 OSPF 进程下未配置 vpn-instance-capability simple 命令的故障处理方式

DN 比特位是否置位	故障处理方式
未配置 **vpn-instance-capability simple**命令，且Network Summary LSA的Option字段包含DN比特位（即DN比特位置位）	根据RFC 2328的规定，私网OSPF进程不会使用DN比特位置位的Network Summary LSA进行路由计算。没有对应的区域间路由是正常现象
未配置 **vpn-instance-capability simple**命令，且Network Summary LSA的Option字段不包含DN比特位	请执行步骤(7)

(6) 检查 ASBR 设备是否可达，检查是否有防环检测。

O_ASE 路由和 O_NSSA 路由是 ASBR 设备发布的，如果本端设备和 ASBR 设备之间路由不可达，则会导致本端设备无法学习到 AS 外部的路由。

a. 请执行 **display ospf** [*process-id*] **lsdb** [**ase** | **nssa**]命令，查看 Adv Rtr 字段，该字段为通告 AS External LSA（Type-5）或 NSSA External LSA（Type-7）的 Router ID，即 ASBR 的 Router ID。

```
<Sysname> display ospf 100 lsdb ase

         OSPF Process 100 with Router ID 1.1.1.1
                 Link State Database


    Type      : External
    LS ID     : 10.1.1.0
    Adv Rtr   : 1.1.1.1
    LS age    : 169
    Len       : 36
```

```
    Options   : O E
    Seq#      : 80000001
    Checksum  : 0x934b
    Net Mask  : 255.255.255.0
    TOS 0  Metric: 1
    E Type    : 2
    Forwarding Address : 192.168.51.5
    Tag       : 1
<Sysname> display ospf 100 lsdb nssa

         OSPF Process 100 with Router ID 1.1.1.1
                       Area: 0.0.0.0
                Link State Database

                       Area: 0.0.0.1
                Link State Database


    Type      : NSSA
    LS ID     : 192.168.51.0
    Adv Rtr   : 5.5.5.5
    LS age    : 156
    Len       : 36
    Options   : O NP
    Seq#      : 80000001
    Checksum  : 0x59dc
    Net Mask  : 255.255.255.0
    TOS 0  Metric: 1
    E Type    : 2
    Forwarding Address : 192.168.51.5
    Tag       : 1

    Type      : NSSA
    LS ID     : 10.1.1.0
    Adv Rtr   : 5.5.5.5
    LS age    : 156
    Len       : 36
    Options   : O NP
    Seq#      : 80000001
    Checksum  : 0xa422
    Net Mask  : 255.255.255.0
    TOS 0  Metric: 1
    E Type    : 2
    Forwarding Address : 192.168.51.5
    Tag       : 1
```

b. 请执行 **`display ospf abr-asbr`** 命令，查看 Destination 字段和 RtType 字段，RtType 字段取值为 ASBR 时，Destination 字段为 ASBR 的 Router ID。查看到此类路由信息时，说明存在到达为 ASBR 的路由。

```
<Sysname> display ospf 100 abr-asbr

         OSPF Process 100 with Router ID 1.1.1.1
                 Routing Table to ABR and ASBR

 Type    Destination     Area            Cost     Nexthop         RtType
 Intra   5.5.5.5         0.0.0.1         1        192.168.51.5    ASBR
```

c. 如果 abr-asbr 信息中不包含到达通告 AS External LSA 或 NSSA External LSA 的 ASBR 的路由，请执行步骤(7)。

d. 如果 abr-asbr 信息中包含到达通告 AS External LSA 或 NSSA External LSA 的 ASBR 的路由，且 LSA 的 Forwarding Address 字段不为零，需要检查 Forwarding Address 的可达性及路由类型。

请在用户视图下执行 **disply ospf routing** *forwarding-address* { *mask-length* | *mask* }命令查询是否存在到达 Forwarding Address 的路由。

```
<Sysname> display ospf 100 routing 192.168.51.5 24

         OSPF Process 100 with Router ID 1.1.1.1
                  Routing Table

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 192.168.51.0/24    1        Transit 0.0.0.0         5.5.5.5         0.0.0.1

 Total nets: 1
 Intra area: 1  Inter area: 0  ASE: 0  NSSA: 0
```

Forwarding Address 的可达性及路由类型对 OSPF 是否能够学习到 O_ASE 路由或 O_NSSA 路由的影响如表 6 所示。

表6 Forwarding Address 的可达性及路由类型对 O_ASE 路由或 O_NSSA 路由的影响

Forward Address 是否可达	故障处理方式
不可达	如果通过**display ospf routing** *forwarding-address* { *mask-length* | *mask* }命令无法查看到路由信息，说明Forwarding Address不可达，请执行步骤(7)
可达	如果外部路由是由NSSA External LSA（Type-7）通告的，根据RFC 3101的规定，要求到达Forwarding Address的路由所在区域与NSSA External LSA所在区域相同。如果Area字段标明的区域号与NSSA External LSA所在的区域不同，OSPF不使用此类NSSA External LSA进行路由计算。因此，没有对应的外部路由是正常现象
	通过**display ospf routing** *forwarding-address* { *mask-length* | *mask* }命令查看到的路由的Type字段为Type1或者Type2，说明到达Forwarding Address的路由类型是外部路由。根据RFC 2328的规定，到达非零Forwarding Address的路由类型不允许是外部路由，OSPF不使用此类LSA进行路由计算。因此，没有对应的外部路由是正常现象

e. 如果 abr-asbr 信息中包含到达通告 AS External LSA 或 NSSA External LSA 的 ASBR 的路由，且本 OSPF 进程绑定了 VPN 实例。

请检查本 OSPF 进程下是否配置了 **vpn-instance-capability simple** 命令。如果 OSPF 进程下配置了 **vpn-instance-capability simple** 命令，请执行步骤(7)。

如果 OSPF 进程下未配置 **vpn-instance-capability simple** 命令，故障处理方式如表 7 所示。

表7 OSPF 进程下未配置 vpn-instance-capability simple 命令的故障处理方式

DN 比特位是否置位	故障处理方式
未配置 **vpn-instance-capability simple**命令，且AS External LSA或者NSSA External LSA的Option字段包含DN比特位	根据RFC 2328的规定，私网OSPF进程不会使用DN比特位置位的AS External LSA或者NSSA External LSA进行路由计算。没有对应的外部路由是正常现象
未配置 **vpn-instance-capability simple**命令，且AS External LSA或者NSSA External LSA的Option字段不包含DN比特位	请执行**display ospf**命令查看Default ASE parameters字段，确认AS External LSA或者NSSA External LSA的Tag值是否与私网OSPF进程的Tag值相同： • 对于 Tag 值相同的情况，根据 RFC 2328 的规定，私网 OSPF 进程不会使用此类 LSA 进行路由计算。因此，没有对应的外部路由是正常现象 • 对于 Tag 值不同的情况，请执行步骤(7)

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

9.4.4 网络中 IP 地址冲突导致路由震荡

1. 故障描述

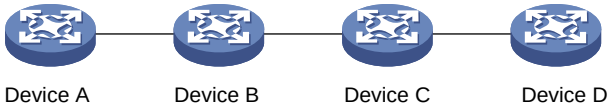
OSPF 组网中不同设备上配置相同的接口 IP 地址，会导致 OSPF 路由震荡。出现此问题时，设备通常伴随如下现象：

- 执行命令 **display cpu-usage** 查看到设备 CPU 使用率较高。
- OSPF 频繁地老化 LSA、重新生成 LSA。
- 设备路由频繁刷新、路由计算出错。

2. 处理步骤

以图 52 为示例说明此类故障的处理方式。其他组网与该组网处理此类故障的思路是相同的。

图52 网络中 IP 地址冲突导致路由震荡组网示例



(2) 在 OSPF 网络中的各个设备上每隔一秒执行一次 **display ospf** [*process-id*] **lsdb** 命令，查看每台设备的 OSPF 链路状态数据库（LSDB）信息。

(3) 检查是否存在 LSA 老化异常的情况。

同时满足如下条件时，说明 LSA 老化异常。

a. 在 Device A 上发现同一个 AdvRouter 通告的 Network LSA（Type-2）的老化时间（Age）非自然增长，一直为最小值，且 Sequence 字段增加很快。例如在如下显示信息中，LinkStateID 为 172.168.0.1 的 Network LSA 的 Age 非自然增长，短时间内 Sequence 从 8000002D 快速增长为 8000002F。

```
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 10.1.1.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         797  48    80000009  0
 Router    1.1.1.1         1.1.1.1         835  36    80000005  0
 Router    4.4.4.4         4.4.4.4         798  36    80000004  0
 Router    10.1.1.1        10.1.1.1        415  36    80000007  0
 Router    2.2.2.2         2.2.2.2         415  48    80000015  0
 Network   192.168.0.2     3.3.3.3         802  32    80000002  0
 Network   172.168.0.3     4.4.4.4         791  32    80000002  0
 Network   172.168.0.1     10.1.1.1        7    32    8000002D  0
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 10.1.1.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         810  48    80000009  0
 Router    1.1.1.1         1.1.1.1         848  36    80000005  0
 Router    4.4.4.4         4.4.4.4         811  36    80000004  0
 Router    10.1.1.1        10.1.1.1        428  36    80000007  0
 Router    2.2.2.2         2.2.2.2         428  48    80000015  0
 Network   192.168.0.2     3.3.3.3         815  32    80000002  0
 Network   172.168.0.3     4.4.4.4         804  32    80000002  0
 Network   172.168.0.1     10.1.1.1        4    32    8000002F  0
```

b. 在 Device B 上相同 Network LSA 的 Age 不断在 3600 和其他较小值之间切换，而且 Sequence 字段增加很快。例如在如下显示信息中，LinkStateID 为 172.168.0.1 的

Network LSA 的 Age 在 3600 和其他较小值之间切换，短时间内 Sequence 从 80000023 快速增长为 80000041。

```
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 2.2.2.2
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         708  48    80000009  0
 Router    1.1.1.1         1.1.1.1         746  36    80000005  0
 Router    4.4.4.4         4.4.4.4         709  36    80000004  0
 Router    10.1.1.1        10.1.1.1        329  36    80000007  0
 Router    2.2.2.2         2.2.2.2         327  48    80000015  0
 Network   172.168.0.3     4.4.4.4         702  32    80000002  0
 Network   192.168.0.2     3.3.3.3         713  32    80000002  0
 Network   172.168.0.1     10.1.1.1        3600 32    80000023  0
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 2.2.2.2
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         748  48    80000009  0
 Router    1.1.1.1         1.1.1.1         786  36    80000005  0
 Router    4.4.4.4         4.4.4.4         749  36    80000004  0
 Router    10.1.1.1        10.1.1.1        369  36    80000007  0
 Router    2.2.2.2         2.2.2.2         367  48    80000015  0
 Network   172.168.0.3     4.4.4.4         742  32    80000002  0
 Network   192.168.0.2     3.3.3.3         753  32    80000002  0
 Network   172.168.0.1     10.1.1.1        7    32    80000041  0
```

c. 在 Device C 上，相同 Network LSA 的 Age 一直为 3600，或者偶尔没有这条 LSA，而且 Sequence 字段增加很快。例如在如下显示信息中，LinkStateID 为 172.168.0.1 的 Network LSA 的 Age 为 3600，或者偶尔没有这条 LSA；存在这条 LSA 时，短时间内 Sequence 从 80000309 增长到 80000346。

```
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 3.3.3.3
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         740  48    8000000D  0
 Router    4.4.4.4         4.4.4.4         759  36    80000008  0
 Router    10.1.1.1        10.1.1.1        364  36    8000000B  0
 Router    2.2.2.2         2.2.2.2         366  48    80000019  0
```

```
 Network   172.168.0.3     4.4.4.4         755  32    80000006  0
 Network   192.168.0.2     3.3.3.3         744  32    80000006  0
 Network   172.168.0.1     10.1.1.1        3600 32    80000309  0
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 3.3.3.3
                 Link State Database

                          Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         745  48    8000000D  0
 Router    4.4.4.4         4.4.4.4         764  36    80000008  0
 Router    10.1.1.1        10.1.1.1        369  36    8000000B  0
 Router    2.2.2.2         2.2.2.2         371  48    80000019  0
 Network   172.168.0.3     4.4.4.4         760  32    80000006  0
 Network   192.168.0.2     3.3.3.3         749  32    80000006  0
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 3.3.3.3
                 Link State Database

                          Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         1302 48    8000000D  0
 Router    4.4.4.4         4.4.4.4         1321 36    80000008  0
 Router    10.1.1.1        10.1.1.1        926  36    8000000B  0
 Router    2.2.2.2         2.2.2.2         928  48    80000019  0
 Network   172.168.0.3     4.4.4.4         1317 32    80000006  0
 Network   192.168.0.2     3.3.3.3         1306 32    80000006  0
 Network   172.168.0.1     10.1.1.1        3600 32    80000346  0
```

(4) 检查是否存在 OSPF 路由震荡。

在 Device B 上每隔一秒执行一次 **display ospf** [*process-id*] **routing** 命令，查看路由是否震荡。

```
<Sysname> display ospf 100 routing

         OSPF Process 100 with Router ID 2.2.2.2
                 Routing Table

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 192.168.0.0/24     1        Transit 0.0.0.0         3.3.3.3         0.0.0.0
 172.168.0.0/24     1        Transit 0.0.0.0         10.1.1.1        0.0.0.0

 Total nets: 2
 Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0
<Sysname> display ospf 100 routing

         OSPF Process 100 with Router ID 2.2.2.2
```

```
                  Routing Table

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 192.168.0.0/24     1        Transit 0.0.0.0         3.3.3.3         0.0.0.0
 172.168.0.0/24     2        Transit 192.168.0.2     4.4.4.4         0.0.0.0

 Total nets: 2
 Intra area: 2  Inter area: 0  ASE: 0  NSSA: 0
```

当 OSPF 路由发生震荡，且多次执行 **display ospf peer** 命令发现邻居关系没有发生震荡时，可以判断该 OSPF 组网中存在 IP 地址冲突。同时，由于 Network LSA（Type-2）是由 DR 发布的，说明产生冲突的设备中有一台设备是 DR。

如果任一台设备上出现两个 LinkState ID 相同的 Network LSA，并且这两个 Network LSA 老化异常。说明产生冲突的设备均为 DR。

```
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 10.1.1.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         367  48    80000021  0
 Router    4.4.4.4         4.4.4.4         369  36    80000013  0
 Router    10.1.1.1        10.1.1.1        477  36    80000012  0
 Router    2.2.2.2         2.2.2.2         403  48    8000002B  0
 Network   192.168.0.1     2.2.2.2         395  32    80000002  0
 Network   172.168.0.1     3.3.3.3         3600 32    8000002B  0
 Network   172.168.0.1     10.1.1.1        9    32    80000036  0
<Sysname> display ospf 100 lsdb

         OSPF Process 100 with Router ID 10.1.1.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter       Age  Len   Sequence  Metric
 Router    3.3.3.3         3.3.3.3         460  48    80000021  0
 Router    4.4.4.4         4.4.4.4         462  36    80000013  0
 Router    10.1.1.1        10.1.1.1        570  36    80000012  0
 Router    2.2.2.2         2.2.2.2         496  48    8000002B  0
 Network   192.168.0.1     2.2.2.2         488  32    80000002  0
 Network   172.168.0.1     3.3.3.3         3600 32    80000034  0
 Network   172.168.0.1     10.1.1.1        6    32    80000041  0
```

(5) 定位产生冲突的设备。

结合 **display ospf lsdb** 的显示信息，找到产生 IP 地址冲突的设备。

- 产生冲突的设备中，仅有一台设备为 DR。

根据异常 Network LSA 的 AdvRouter，可以找到产生该 Network LSA 的 DR 设备；然后根据 Network LSA 中的 LinkState ID 找到产生 IP 地址冲突的接口，确定该接口的 IP 地址。根据接口的 IP 地址以及网络 IP 地址规划，找到另外一台产生冲突的设备。

在本例中，可以判断 Router ID 为 10.1.1.1 的 DR 设备接口 IP 地址与其他设备接口 IP 地址冲突，产生冲突的 IP 地址是 172.168.0.1。然后根据网络 IP 地址规划，找到与 DR 设备接口 IP 地址冲突的另外一台设备。

- 产生冲突的设备均为 DR。

  根据异常 Network LSA 的 AdvRouter，可以找到产生该 Network LSA 的 DR 设备；然后根据 Network LSA 中的 LinkState ID 找到产生 IP 地址冲突的接口。

(6) 根据网络 IP 地址规划修改冲突一方的 IP 地址。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

3. 告警与日志

相关告警

无

相关日志

无

10 组播类故障处理

10.1 MSDP故障处理

10.1.1 MSDP 对等体无法正确建立（S，G）表项

1. 故障描述

配置组播网络后发现 MSDP 对等体无法正确建立（S，G）表项。

2. 常见原因

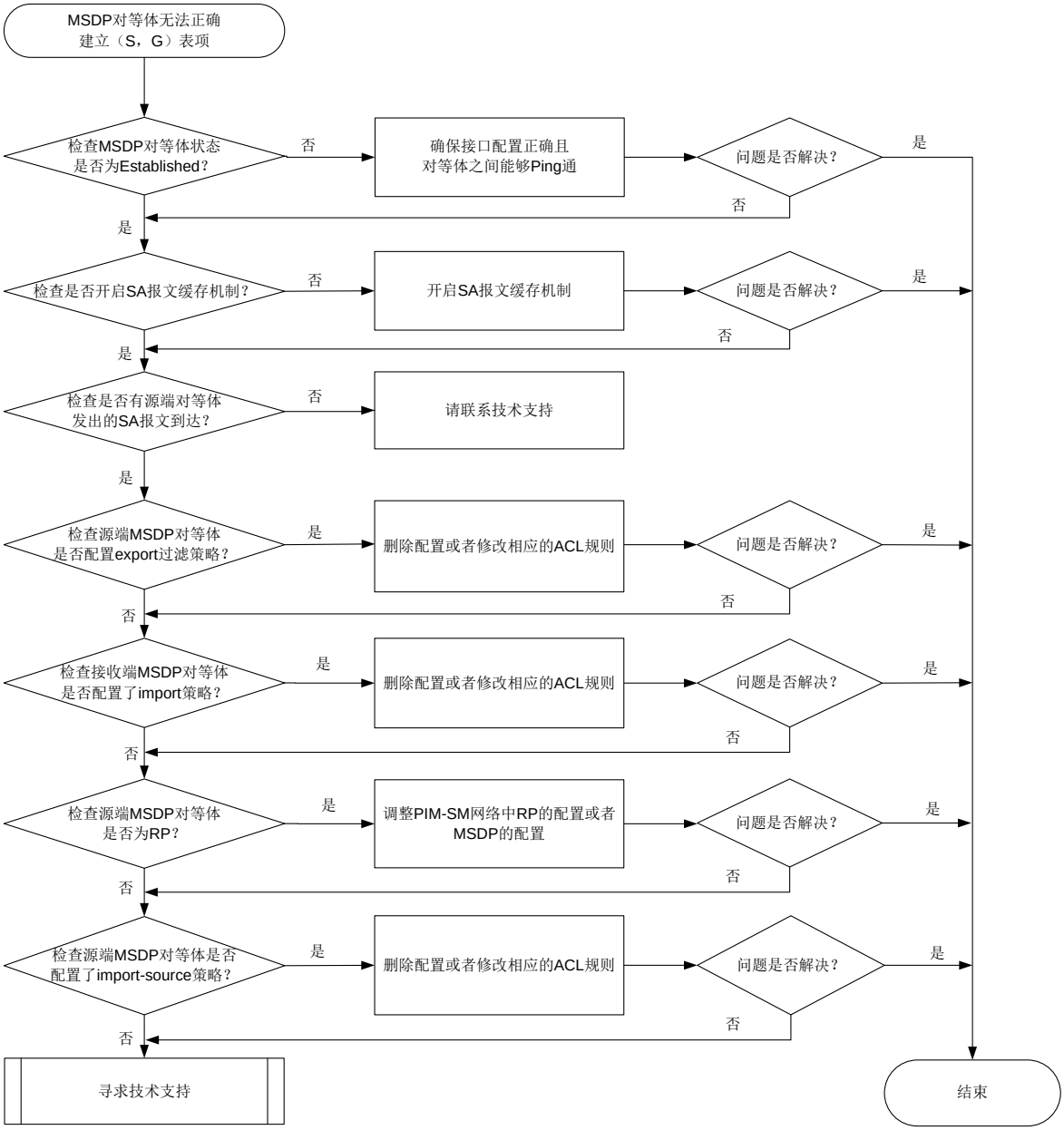
本类故障的常见原因主要包括：

- MSDP 对等体建立失败。
- SA 报文缓存机制未开启。
- 没有收到源端对等体发出的 SA 报文。
- 创建 SA 报文的 MSDP 对等体没有部署在 RP 上。
- 配置问题（比如，export、import 过滤策略、import-source 策略配置不正确）。

3. 故障分析

本类故障的诊断流程如图 53 所示。

图53 MSDP 对等体无法正确建立（S，G）表项的故障诊断流程图



4. 处理步骤

(1) 检查 MSDP 对等体状态是否为 Established。

在配置了 MSDP 对等体的设备上执行 **display msdp brief** 命令，通过显示信息中的 State 字段判断 MSDP 对等体状态是否为 Established。

a. 如果不是，请检查 MSDP 对等体接口配置是否正确，以及 MSDP 对等体之间是否能够 Ping 通。如果 Ping 不通，请参见“Ping 不通的定位思路”继续定位，确保 MSDP 对等体之间能够 Ping 通。

b. 如果是，请执行步骤(2)。

(2) 检查是否开启 SA 报文缓存机制。

在 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看是否已通过 **cache-sa-enable** 命令开启了 SA 报文缓存机制。

- 如果未开启，请通过 MSDP 视图下的 **cache-sa-enable** 命令开启。
- 如果已开启，请执行步骤(3)。

(3) 检查是否有源端对等体发出的 SA 报文到达。

在 MSDP 对等体上执行 **display msdp sa-cache** 命令，查看本设备上 SA 缓存中（S，G）表项的信息。通过查看是否存在相应的表项信息，判断对等体是否收到源端对等体发送的 SA 报文。

- 如果未收到，请执行步骤(4)。
- 如果已收到，请执行步骤(8)。

(4) 检查源端 MSDP 对等体是否配置 export 过滤策略。

在源端 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看设备上是否已通过 **peer** *peer-address* **sa-policy export** 命令配置 export 策略，即是否配置对转发给指定 MSDP 对等体的 SA 报文进行过滤。

- 如果已配置，根据是否通过 **acl** 命令配置过滤规则，分为如下两种情况处理：
  - 如果未配置 ACL 过滤规则，则表示该 MSDP 对等体不转发 SA 报文，请执行 **undo peer peer-address sa-policy export** 命令删除该配置。
  - 如果配置了 ACL 过滤规则，则表示该 MSDP 对等体只转发符合 ACL 规则的（S，G）表项的 SA 报文。请检查需要转发的（S，G）表项的 SA 报文能否通过已配置的 ACL 规则的过滤。如果不能，可以执行 **undo peer peer-address sa-policy export** 命令删除该配置或调整指定的 ACL 规则。
- 如果未配置，请执行步骤(5)。

(5) 检查接收端 MSDP 对等体是否配置了 import 策略。

在接收端 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看设备上是否已通过 **peer** *peer-address* **sa-policy import** 命令配置 import 策略，即对来自指定 MSDP 对等体的 SA 报文进行过滤。

- 如果已配置，根据是否通过 **acl** 命令配置过滤规则，分为如下两种情况处理：
  - 如果未配置 ACL 过滤规则，则表示该 MSDP 对等体不接收任何 SA 报文，请执行 **undo peer peer-address sa-policy import** 命令删除该配置。
  - 如果配置了 ACL 过滤规则，则表示该 MSDP 对等体只接收符合 ACL 规则的（S，G）表项的 SA 报文。请检查需要接收的（S，G）表项的 SA 报文能否通过已配置的 ACL 规则的过滤。如果不能，可以执行 **undo peer peer-address sa-policy import** 命令删除该配置或调整指定的 ACL 规则。
- 如果未配置，请执行步骤(6)。

(6) 检查源端 MSDP 对等体是否为 RP。

在源端 MSDP 对等体上执行 **display pim routing-table** 命令，通过查看显示信息中（S，G）对应的 Flag 字段取值是否为 2MSDP，判断该 MSDP 对等体是否为 RP。

- 如果不是，请调整 PIM-SM 网络中 RP 的配置或者远端 MSDP 对等体的配置，确保源端 MSDP 对等体为 RP。
- 如果是，请执行步骤(7)。

(7) 检查源端 MSDP 对等体是否配置了 import-source 策略。

在源端 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看设备上是否已通过 **import-source** 命令配置了 SA 报文的创建规则。

- 如果已配置，根据是否通过 **acl** 命令配置过滤规则，分为如下两种情况处理：
  - 如果未配置 ACL 过滤规则，则表示该 MSDP 对等体在创建 SA 报文时，对所有的（S，G）表项不作通告，请执行 **undo import-source** 命令删除该配置。
  - 如果配置了 ACL 过滤规则，则表示该 MSDP 对等体在创建 SA 报文时，只通告符合 ACL 规则的（S，G）表项。请检查需要通告的（S，G）表项能否通过已配置的 ACL 规则的过滤。如果不能，可以执行 **undo import-source** 命令删除该配置或调整指定的 ACL 规则。
- 如果未配置，请执行步骤(8)。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

10.2 PIM故障处理

10.2.1 PIM 邻居 Down

1. 故障描述

PIM 邻居 Down。

2. 常见原因

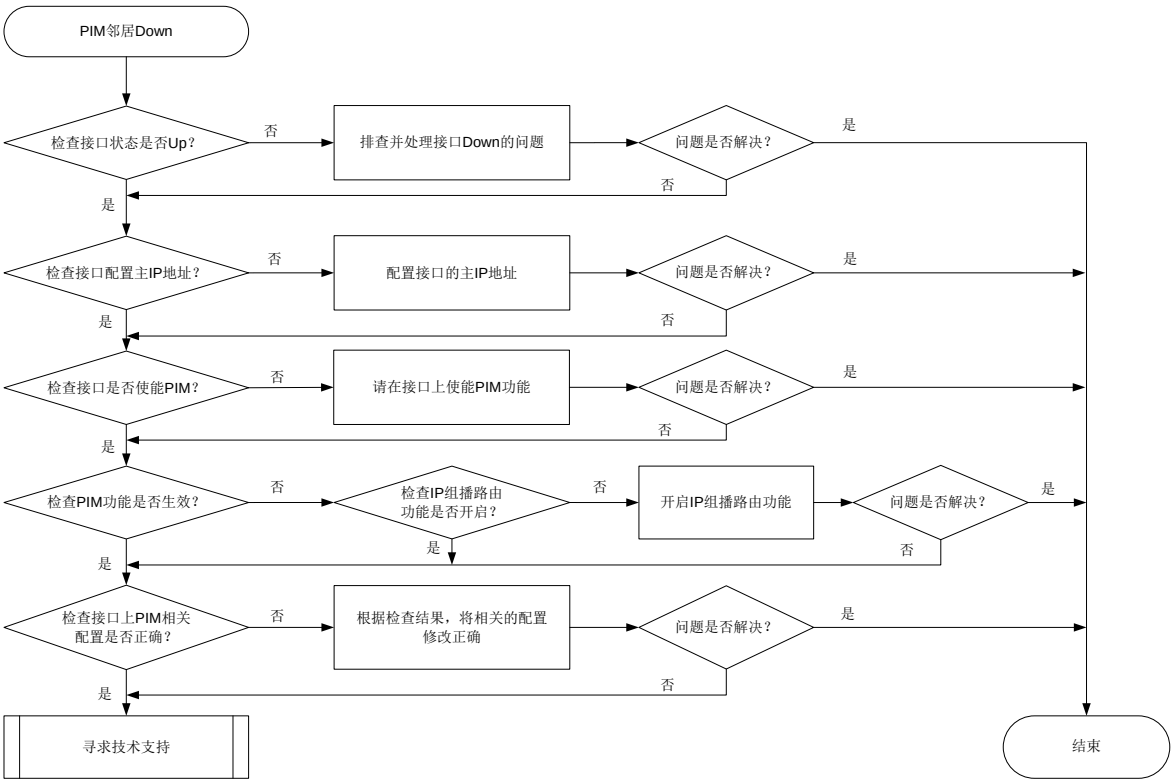
本类故障的常见原因主要包括：

- 接口物理状态为 Down。
- 接口上未配置主 IP 地址。
- 接口上 PIM 功能没有生效。
- 接口没有使能 PIM。
- 接口上 PIM 相关配置不正确。

3. 故障分析

本类故障的诊断流程如图 54 所示。

图54 PIM 邻居 Down 的故障诊断流程图



4. 处理步骤

(1) 检查接口的物理状态是否为 Up。

请在设备上执行 **display interface** *interface-type interface-number* 命令查看显示信息中的“Current state”字段，确认接口的物理状态是否为 Up。

a. 如果为 Up，请执行步骤(2)。

b. 如果为 Down，请排查处理接口物理 Down 的问题。

(2) 检查接口上是否配置了主 IP 地址。

在设备直连用户主机网段接口的接口视图下执行 **display this** 命令，查看是否通过 **ip address** 命令配置了接口的主 IP 地址。

a. 如果没有配置，请在接口上通过 **ip address** 命令进行配置。

b. 如果已配置，请执行步骤(3)。

(3) 检查接口是否使能 PIM。

在设备上执行 **display current-configuration interface** 命令，查看接口上是否使能 PIM。

a. 如果没有使能，请在接口视图下执行 **pim dm** 或 **pim sm** 命令开启 PIM 功能。

b. 如果已使能，请执行步骤(4)。

(4) 检查接口 PIM 功能是否生效。

在设备上执行 **display pim interface** 命令，通过查看显示信息中是否存在该接口对应的 PIM 相关信息确认接口上 PIM 功能是否生效。

a. 如果没有生效，请在设备上执行 **display current-configuration | include multicast** 命令，查看是否开启 IP 组播路由功能。
   - 如果没有开启，请在系统视图下执行 **multicast routing** 命令开启 IP 组播路由功能。
   - 如果已开启，请执行步骤(5)。

b. 如果已生效，请执行步骤(5)。

(5) 检查接口上 PIM 相关配置是否正确。

在接口上因配置错误导致无法建立 PIM 邻居的常见原因如下：

- 直连接口的 IP 地址有没有配置在同一网段内，请将需要建立 PIM 邻居的设备直连口的 IP 地址配置在同一网段内。
- 接口上通过 **pim neighbor-policy** 命令配置了 Hello 报文过滤器，但 PIM 邻居 IP 地址不在 ACL 的 permit 规则中，接口发送的 Hello 报文被当作非法报文过滤掉，从而建立邻居失败。请确认是否需要配置 Hello 报文过滤器：
  - 如果需要，请修改 ACL 配置，使得 PIM 邻居的 IP 地址在 ACL 的 permit 规则中。
  - 如果不需要，请执行 **undo pim neighbor-policy** 命令删除对 Hello 报文的过滤规则。
- 接口上通过 **pim require-genid** 命令配置了拒绝无 Generation ID 的 Hello 报文功能，而 PIM 邻居发送的 Hello 报文中未携带 Generation ID，导致 PIM 邻居无法建立。请确认是否需要配置拒绝无 Generation ID 的 Hello 报文功能：
  - 如果需要，请执行步骤(6)。
  - 如果不需要，请在设备上执行 **undo pim require-genid** 命令删除此配置。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

10.2.2 PIM 域内三层组播流量不通

1. 故障描述

开启 IP 组播路由功能后，同一 PIM 域内三层组播流量不通。

2. 常见原因

本类故障的常见原因主要包括：

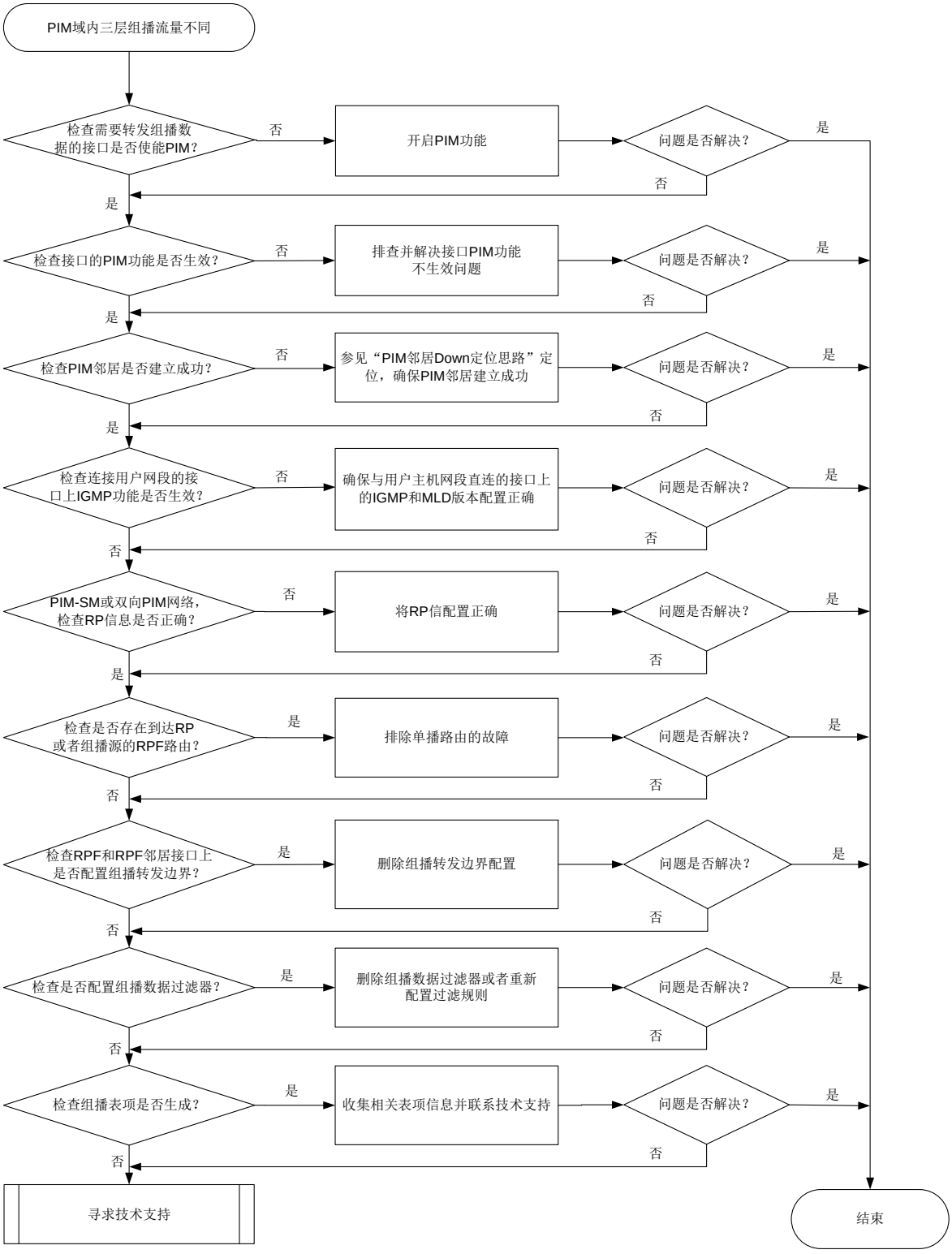
- 需要转发组播数据的接口未使能 PIM。
- 接口的 PIM 协议没有生效。
- PIM 邻居未建立成功。

- 连接用户网段的接口未使能 IGMP。
- 在 PIM-SM 或双向 PIM 网络中，没有配置 RP 或 RP 信息不正确。
- 不存在到达 RP 或组播源的 RPF 路由。
- 转发组播数据的接口上配置了组播边界。
- 在 PIM-SM 或双向 PIM 网络中，配置了错误的组播源过滤策略。
- 组播表项未生成。

3. 故障分析

本类故障的诊断流程如图 55 所示。

图55 PIM 域内三层组播流量不通的故障诊断流程图



4. 处理步骤

(1) 检查需要转发组播数据的接口是否使能 PIM。

在需要转发组播数据的接口视图下执行 **display this** 命令，检查是否存在 **pim sm** 或 **pim dm** 的配置。

- 如果不存在，表明接口下 PIM 功能未开启。请在接口视图下通过 **pim sm** 或 **pim dm** 命令开启 PIM 功能。若是双向 PIM 网络，在接口视图下配置了通过 **pim sm** 命令开启 PIM 功能后，还需在 PIM 视图下通过 **bidir-pim enable** 命令开启双向 PIM 功能。
- 如果存在，请执行步骤(2)。

(2) 检查接口的 PIM 功能是否生效。

在设备上执行 **display pim interface** 命令，通过查看显示信息中是否存在该接口对应的 PIM 相关信息确认接口上 PIM 功能是否生效。

- 如果没有生效，请在设备上执行 **display interface** *interface-type interface-number* 命令查看显示信息中的“Current state”字段，确认接口的物理状态是否为 Up。如果为 Down，请排查处理接口物理 Down 的问题。
- 如果生效，请执行步骤(3)。

(3) 检查 PIM 邻居是否建立成功。

在设备上执行 **display pim neighbor** 命令，根据是否存在相应的 PIM 邻居信息，判断 PIM 邻居是否建立成功。

a. 如果未建立成功，请参见“PIM 邻居 Down”进行定位，确保 PIM 邻居建立成功。

b. 如果建立成功，请执行步骤(4)。

(4) 检查连接用户网段的接口上 IGMP 功能是否生效。

在设备上执行 **display igmp interface** 命令，根据是否存在显示信息确认接口 IGMP 功能是否生效。

- 如果没有生效，请检查接口下是否通过 **igmp enable** 命令开启了 IGMP 功能，确保 IGMP 功能已开启。
- 如果已生效，根据不同的网络类型执行如下操作：
  - 若为 PIM-SM 或双向 PIM 网络，请执行步骤(5)。
  - 若为 PIM-DM 网络，请执行步骤(7)。

(5) 对于 PIM-SM 或双向 PIM 网络，检查 RP 信息是否正确。

在设备上执行 **display pim rp-info** 命令，查看设备是否生成了为某组播组服务的 RP 信息表项，并检查 PIM-SM 或双向 PIM 域中其它所有设备上，为此组播组服务的 RP 信息是否配置一致。

- 如果不一致，且 PIM-SM/双向 PIM 网络中使用静态 RP，请在 PIM-SM/双向 PIM 域的所有设备上的 PIM 视图下执行 **static-rp** 命令，将为某组播组服务的 RP 地址配置为相同的地址；如果 PIM-SM/双向 PIM 网络中使用动态 RP，请执行步骤(6)。
- 如果一致，请执行步骤(6)。

(6) 检查是否存在到达 RP 的 RPF 路由。

在设备上执行 **display multicast rpf-info** 命令，查看是否存在到达 RP 的 RPF 路由。

- 如果不存在，检查单播路由配置。请在当前设备和 RP 上分别执行 **ping** 命令，检查是否能够互相 ping 通。如果 ping 不通，请修改单播路由配置，直到 ping 通为止。
- 如果存在，通过执行 **display multicast rpf-info** 命令，查看显示信息中的 Referenced route type 字段，确认 RPF 为组播静态路由还是单播路由。

- 如果 RPF 路由为组播静态路由，请执行 **display multicast routing-table static** 命令查看组播静态路由配置是否合理。
- 如果 RPF 路由为单播路由，请执行 **display ip routing-table** 命令查看单播路由是否与 RPF 路由一致。

如果到达 RP 的 RPF 路由存在且配置合理，请执行步骤(8)。

(7) 检查是否存在到达组播源的 RPF 路由。

在设备上执行 **display multicast rpf-info** 命令，查看是否存在到达组播源的 RPF 路由。

- 如果不存在，检查单播路由配置。请在当前设备和组播源上分别执行 **ping** 命令，检查是否能够互相 ping 通。如果 ping 不通，请修改单播路由配置，直到 Ping 通为止。
- 如果存在，通过执行 **display multicast rpf-info** 命令，查看显示信息中的 Referenced route type 字段，确认 RPF 为组播静态路由还是单播路由。
  - 如果 Referenced route type 字段显示为“multicast static”，表示 RPF 路由为组播静态路由，请执行 **display multicast routing-table static** 命令查看组播静态路由配置是否合理。
  - 如果 Referenced route type 字段显示为“igp”、“egp”、“unicast (direct)”或“unicast”，表示 RPF 路由为单播路由，请执行 **display ip routing-table** 命令查看单播路由是否与 RPF 路由一致。

如果到达组播源的 RPF 路由存在且配置合理，请执行步骤(8)。

(8) 检查 RPF 接口和 RPF 邻居接口上是否配置组播转发边界。

在设备上执行 **display multicast boundary** 命令，查看接口上是否配置了组播转发边界。

- 如果已配置，建议在接口上执行 **undo multicast boundary** 命令删除对应配置或重新进行网络规划，确保 RPF 接口和 RPF 邻居接口没有配置组播边界。
- 如果未配置，请执行步骤(9)。

(9) 检查是否配置组播数据过滤器。

在 PIM 视图下执行 **display this** 命令，查看是否配置组播数据过滤器（通过 PIM 视图下的 **source-policy** 命令配置）。

- 如果已配置，继续确认接收到的组播数据是否在过滤器指定的允许范围之内。如果不在，建议根据实际组网需要执行 **undo source-policy** 命令删除该配置或重新配置 ACL 规则，确保用户需要的组播数据正常转发。
- 如果未配置，请执行步骤(10)。

(10) 检查组播表项是否生成。

在设备上分别查看组播表项是否生成：

- 如果存在相应的表项，流量仍然不通，请收集相关表项信息，并执行步骤(11)。
- 如果不存在，请执行步骤(11)。

需要查看的组播表项以及查看方式如下：

- 在设备上执行 **display pim routing-table** 命令，检查 PIM 协议路由表项是否生成。
- 在设备上执行 **display igmp group** 命令，检查 IGMP 协议是否有对应的组播组。
- 在设备上执行 **display multicast routing-table** 命令，检查组播路由表是否生成。

- 在设备上执行 **display multicast forwarding-table** 命令，检查组播转发表是否生成。

(11) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

10.2.3 PIM-SM 网络中 SPT 无法正常转发数据

1. 故障描述

PIM-SM 网络中 SPT 无法正常转发数据，组播流量不通。

2. 常见原因

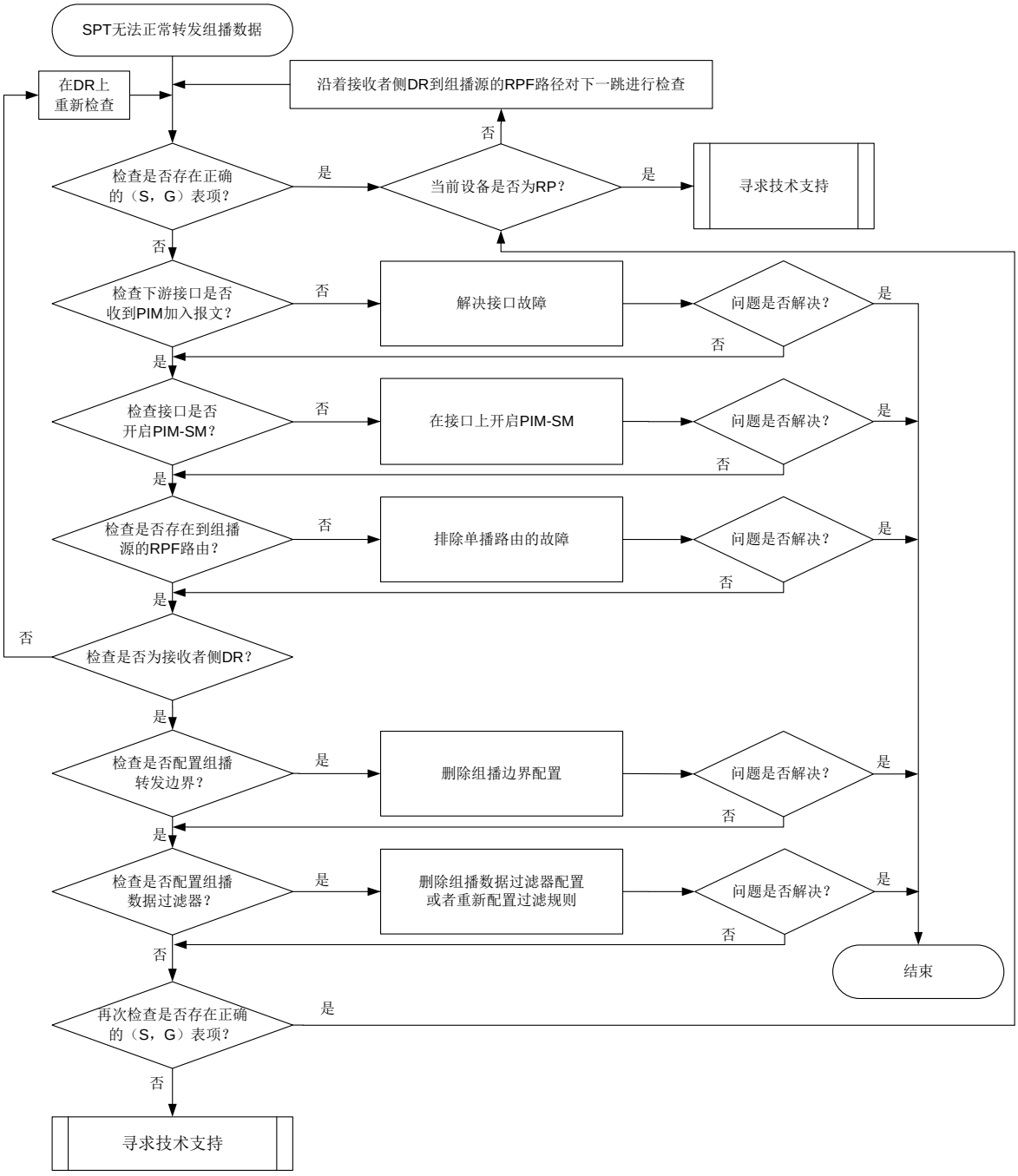
本类故障的常见原因主要包括：

- 组播设备连接下游设备的接口没有收到 PIM 加入报文。
- PIM-SM 域内组播设备上的接口没有开启 PIM-SM。
- PIM-SM 域内组播设备到组播源的 RPF 路由不正确。
- 配置不正确（比如组播转发边界配置不正确、组播数据过滤器配置不正确等）。

3. 故障分析

本类故障的诊断流程如图 56 所示。

图56 PIM-SM 网络中 SPT 无法正常转发数据故障诊断流程图



4. 处理步骤

(1) 检查 PIM 路由表中是否存在正确的（S，G）表项。

在设备上执行 **display pim routing-table** 命令，查看 PIM 路由表中是否存在正确的（S，G）表项。如果 PIM 路由表中存在正确的（S，G）表项，查看下游接口列表中是否包含到达所有组成员的下游接口。

- 如果 PIM 路由表中的（S，G）表项存在且信息完全正确，请在设备上执行 **display multicast forwarding-table** 命令，通过显示信息中的“Matched packets”和

“Forwarded packets”字段，确认（S，G）表项匹配的组播报文数量和已转发的组播报文是否保持增长。如果转发表中不存在(S,G)表项或(S,G)表项对应的“Matched packets”字段值是否停止增长，则表示上游设备转发给此设备的组播数据不正常。此时，需要判断当前设备是否为组播源侧 DR：

- 如果不是，则表示当前设备没有收到组播数据，故障可能出在上游设备，请检查上游设备的 PIM 路由表中是否存在正确的（S，G）表项。如果上游设备的 PIM 路由表中存在正确的（S，G）表项，但是“Matched packets”统计的组播报文数量停止增长，请执行步骤(9)。
- 如果是，则表示 SPT 已成功建立，但由于某种原因导致组播源侧 DR 未沿着 SPT 转发组播数据，请执行步骤(9)。

- 如果 PIM 路由表中不存在正确的（S，G）表项，请执行步骤(2)。

(2) 检查连接下游设备的接口是否收到 PIM 加入报文。

联系技术支持，在专业人士的指导下使用抓包工具（例如 Wireshark）在设备连接下游设备的接口上进行抓包，查看连接下游设备接口是否收到 PIM 加入/剪枝报文。

- 如果没有收到 PIM 加入/剪枝报文，则在下游设备连接本设备的接口上，使用抓包工具（例如 Wireshark）进行抓包，查看是否发送 PIM 加入/剪枝报文给本设备。如果下游设备没有发送 PIM 加入/剪枝报文，则表示下游设备存在问题，请排查下游设备故障。如果下游设备已经发送 PIM 加入/剪枝报文，但是本设备没有收到，则表示与本设备之间 PIM 邻居通信有问题，请执行步骤(9)。
- 如果连接下游设备接口收到了 PIM 加入/剪枝报文，请执行步骤(3)。

(3) 检查接口是否开启 PIM-SM。

在当前设备上执行 **display pim interface verbose** 命令，查看接口上的 PIM 信息。

a. 重点查看到达组播源的 RPF 邻居接口、到达组播源的 RPF 接口和直连用户主机网段的接口(接收者侧 DR 的下游接口)上的 PIM 相关配置信息。如果这些接口上没有开启 PIM-SM，请通过 **pim sm** 命令开启。同时，检查确保设备上已使能 IP 组播路由（通过 **multicast routing** 命令配置）且 PIM 邻居建立成功（通过 **display pim neighbor** 命令查看）。

b. 如果设备上述重点查看的接口都开启了 PIM-SM，但问题依然存在，请执行步骤(4)。

(4) 检查是否存在到达组播源的 RPF 路由。

在设备上执行 **display multicast rpf-info** 命令，查看是否存在到达组播源的 RPF 路由。

- 如果不存在，检查单播路由配置。请在当前设备和组播源上分别执行 **ping** 命令，检查是否能够互相 ping 通。如果 ping 不通，请修改单播路由配置，直到 Ping 通为止。
- 如果存在，通过执行 **display multicast rpf-info** 命令，查看显示信息中的 Referenced route type 字段，确认 RPF 为组播静态路由还是单播路由。
  - 如果 Referenced route type 字段显示为“multicast static”，表示 RPF 路由为组播静态路由，请执行 **display multicast routing-table static** 命令查看组播静态路由配置是否合理。
  - 如果 Referenced route type 字段显示为“igp”、“egp”、“unicast (direct)”或“unicast”，表示 RPF 路由为单播路由，请执行 **display ip routing-table** 命令查看单播路由是否与 RPF 路由一致。

如果到达组播源的 RPF 路由存在且配置合理，请执行步骤(5)。

(5) 检查转发组播数据的接口对应的 DR 是否为接收者侧 DR。

在设备上执行 **display pim interface** 命令，查看转发组播数据的接口对应的 DR 是否为接收者侧 DR。判断方法为查看显示信息中 DR-Address 字段是否携带 local 标记，如果携带，则为接收者侧 DR。

- 如果不是接收者侧 DR，请根据显示信息中的 DR 地址找到对应的 DR 设备，并在该 DR 设备上执行步骤(6)。
- 如果是接收者侧 DR，请在当前设备上执行步骤(6)。

(6) 检查 RPF 接口和 RPF 邻居接口上是否配置组播转发边界。

在设备上执行 **display multicast boundary** 命令，查看接口上是否配置了组播转发边界。

- 如果已配置，建议在接口上执行 **undo multicast boundary** 命令删除对应配置或重新进行网络规划，确保 RPF 接口和 RPF 邻居接口没有配置组播边界。
- 如果未配置，请执行步骤(7)。

(7) 检查是否配置组播数据过滤器。

在 PIM 视图下执行 **display this** 命令，查看是否配置组播数据过滤器（通过 PIM 视图下的 **source-policy** 命令配置）。

- 如果已配置，继续确认接收到的组播数据是否在过滤器指定的允许范围之内。如果不在，建议根据实际组网需要执行 **undo source-policy** 命令删除该配置或重新配置 ACL 规则，确保用户需要的组播数据正常转发。
- 如果未配置，请执行步骤(8)。

(8) 再次检查 PIM 路由表是否存在正确的（S，G）表项。

在设备上再次执行 **display pim routing-table** 命令，查看 PIM 路由表中是否存在（S，G）表项。具体方法请参见步骤(1)。

(9) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

10.2.4 PIM-SM 网络中 RPT 无法正常转发数据

1. 故障描述

PIM-SM 网络中 RPT 无法正常转发数据，组播流量不通。

2. 常见原因

本类故障的常见原因主要包括：

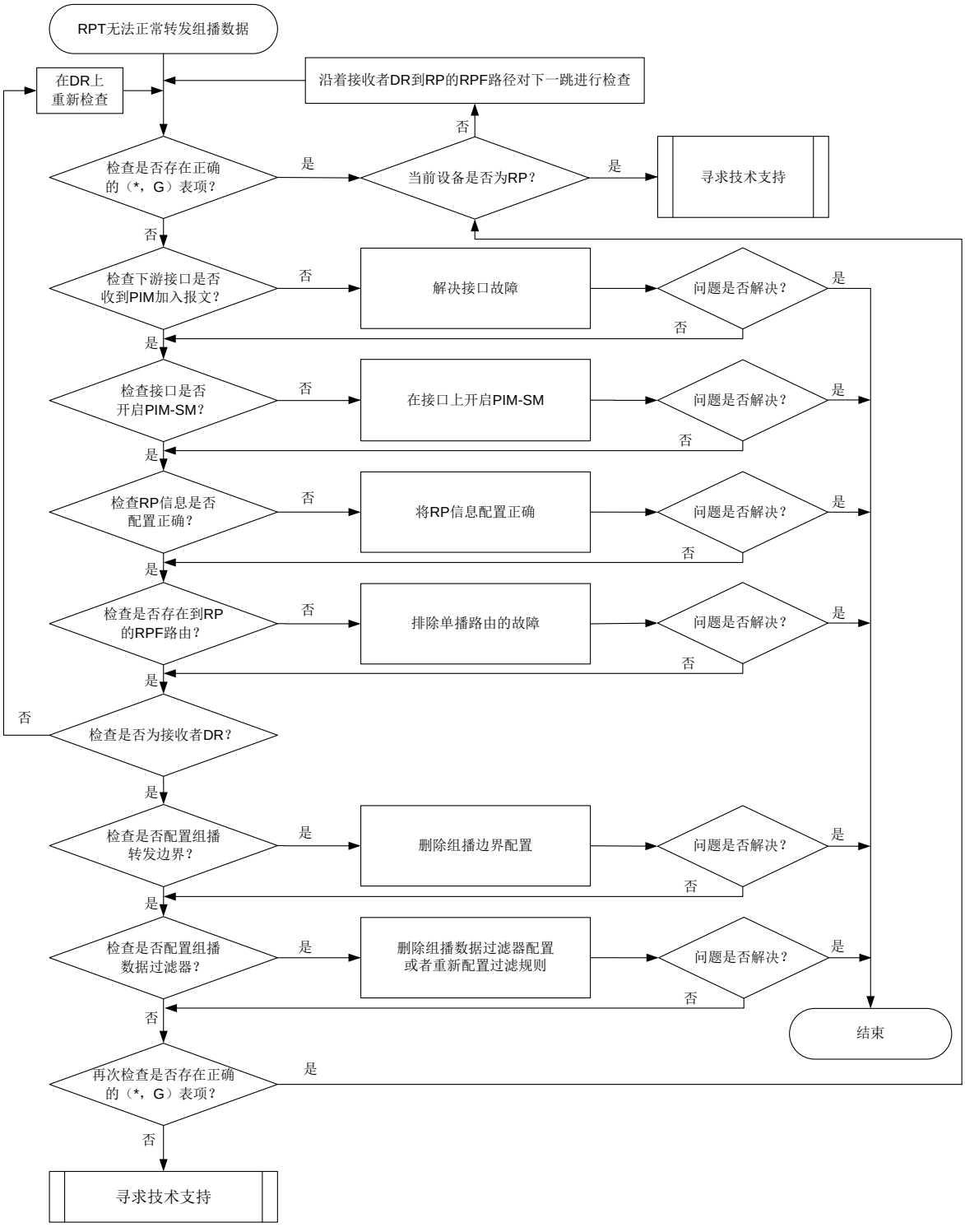
- PIM-SM 域内组播设备到 RP 的单播路由不通。

- PIM-SM 域内各组播设备上为某一组播组服务配置的 RP 地址不一致。
- PIM-SM 域内组播设备的下游接口没有收到 PIM 加入报文。
- PIM-SM 域内组播设备上的接口没有开启 PIM-SM。
- PIM-SM 域内组播设备到 RP 的 RPF 路由不正确。
- 配置不正确（比如组播转发边界配置不正确、组播数据过滤器配置不正确等）。

3. 故障分析

本类故障的诊断流程如图 57 所示。

图57 PIM-SM 网络中 RPT 无法正常转发数据故障诊断流程图



4. 处理步骤

(1) 检查 PIM 路由表中是否存在正确的（*，G）表项。

在设备上执行 **display pim routing-table** 命令，查看 PIM 路由表中是否存在正确的（*，G）表项。请检查下游接口列表中，是否包含到达所有连接（*，G）组成员的下游接口。

- 如果 PIM 路由表中的（*，G）表项存在且信息完全正确，则建议每隔 15 秒执行一次 **display multicast forwarding-table** 命令，查看组播转发表中是否存在与（*，G）表项相同组播组的（S，G）表项，同时查看（S，G）表项匹配的报文数量是否保持增长。如果转发表中不存在（S，G）表项或（S，G）表项匹配的报文数量停止增长，则表示上游设备转发给此设备的组播数据不正常。此时，需要判断当前设备是否为 RP：
  - 如果不是，则表示当前设备没有收到组播数据，故障可能出在上游设备，请检查上游设备的 PIM 路由表中是否存在正确的（S，G）表项。
  - 如果是，则表示 RPT 已成功建立，但由于某种原因（例如源 DR 没有注册成功）导致 RP 未收到组播源发出的组播数据。此时，需要寻求技术支持排除故障。
- 如果 PIM 路由表中不存在正确的（*，G）表项，请执行步骤(2)。

(2) 检查连接下游设备的接口是否收到 PIM 加入报文。

联系技术支持，在专业人士的指导下使用抓包工具（例如 Wireshark）在设备连接下游设备的接口上进行抓包，查看连接下游设备接口是否收到 PIM 加入/剪枝报文。

- 如果没有收到 PIM 加入/剪枝报文，则在下游设备连接本设备的接口上，使用抓包工具（例如 Wireshark）进行抓包，查看是否发送 PIM 加入/剪枝报文给本设备。如果下游设备没有发送 PIM 加入/剪枝报文，则表示下游设备存在问题，请排查下游设备故障。如果下游设备已经发送 PIM 加入/剪枝报文，但是本设备没有收到，则表示与本设备之间 PIM 邻居通信有问题，请执行步骤(10)。
- 如果连接下游设备接口收到了 PIM 加入/剪枝报文，请执行步骤(3)。

(3) 检查接口是否开启 PIM-SM。

在当前设备上执行 **display pim interface verbose** 命令，查看接口上的 PIM 信息。

a. 重点查看到达 RP 的 RPF 邻居接口、到达 RP 的 RPF 接口和直连用户主机网段的接口（接收者侧 DR 的下游接口）上的 PIM 相关配置信息。如果这些接口上没有开启 PIM-SM，请通过 **pim sm** 命令开启。同时，检查设备上是否使能 IP 组播路由（通过 **multicast routing** 命令配置）、PIM 邻居是否建立成功（通过 **display pim neighbor** 命令查看）。

b. 如果设备上述重点查看的接口都开启了 PIM-SM，请执行步骤(4)。

(4) 检查 RP 信息是否正确。

在设备上执行 **display pim rp-info** 命令，查看设备上是否生成了为某个组播组服务的 RP 信息表项，并检查 PIM-SM 域中其它所有设备上，为此组播组服务的 RP 信息是否配置一致。

- 如果不一致，且 PIM-SM 网络中使用静态 RP，请在 PIM-SM 域的所有设备上的 PIM 视图下执行 **static-rp** 命令，将为某组播组服务的 RP 地址配置为相同的地址；如果 PIM-SM 网络中使用动态 RP，请执行步骤(10)。
- 如果一致，请执行步骤 10.2.2 4. (6)。

(5) 检查是否存在到达 RP 的 RPF 路由。

在设备上执行 **display multicast rpf-info** 命令，查看是否存在到达 RP 的 RPF 路由。

- 如果不存在，检查单播路由配置。请在当前设备和 RP 上分别执行 **ping** 命令，检查是否能够互相 ping 通。如果 ping 不通，请修改单播路由配置，直到 ping 通为止。
- 如果存在，通过执行 **display multicast rpf-info** 命令，查看显示信息中的 Referenced route type 字段，确认 RPF 为组播静态路由还是单播路由。

- 如果 RPF 路由为组播静态路由，请执行 **display multicast routing-table static** 命令查看组播静态路由配置是否合理。
- 如果 RPF 路由为单播路由，请执行 **display ip routing-table** 命令查看单播路由是否与 RPF 路由一致。

如果到达 RP 的 RPF 路由存在且配置合理，请执行步骤(6)。

(6) 检查转发组播数据的接口对应的 DR 是否为接收者侧 DR。

在设备上执行 **display pim interface** 命令，查看转发组播数据的接口对应的 DR 是否为接收者侧 DR。判断方法为查看显示信息中 DR-Address 字段是否携带 local 标记，如果携带，则为接收者侧 DR。

- 如果不是接收者侧 DR，请根据显示信息中的 DR 地址找到对应的 DR 设备，并在该 DR 设备上执行步骤(7)。
- 如果是接收者侧 DR，请在当前设备上执行步骤(7)。

(7) 检查 RPF 接口和 RPF 邻居接口上是否配置组播转发边界。

在设备上执行 **display multicast boundary** 命令，查看接口上是否配置了组播转发边界。

- 如果已配置，建议在接口上执行 **undo multicast boundary** 命令删除对应配置或重新进行网络规划，确保 RPF 接口和 RPF 邻居接口没有配置组播边界。
- 如果未配置，请执行步骤(8)。

(8) 检查是否配置组播数据过滤器。

在 PIM 视图下执行 **display this** 命令，查看是否配置组播数据过滤器（通过 PIM 视图下的 **source-policy** 命令配置）。

- 如果已配置，继续确认接收到的组播数据是否在过滤器指定的允许范围之内。如果不在，建议根据实际组网需要执行 **undo source-policy** 命令删除该配置或重新配置 ACL 规则，确保用户需要的组播数据正常转发。
- 如果未配置，请执行步骤(9)。

(9) 再次检查 PIM 路由表是否存在正确的（*，G）表项。

在设备上再次执行 **display pim routing-table** 命令，查看 PIM 路由表中是否存在（*，G）表项。具体方法请参见步骤(1)。

(10) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

10.3 二层组播故障处理

10.3.1 二层组播业务不通

1. 故障描述

二层组播业务不通主要表现在二层组播转发表项无法生成，导致组播流量无法正常转发。

2. 常见原因

本类故障的常见原因主要包括：

- 设备没有收到二层组播协议报文。
- IGMP 协议报文格式不正确。
- 二层组播转发表项未生成。

3. 故障分析

本类故障的诊断思路如下：

(1) 检查是否生成二层组播转发表项。

(2) 检查是否正常收到组播协议报文。

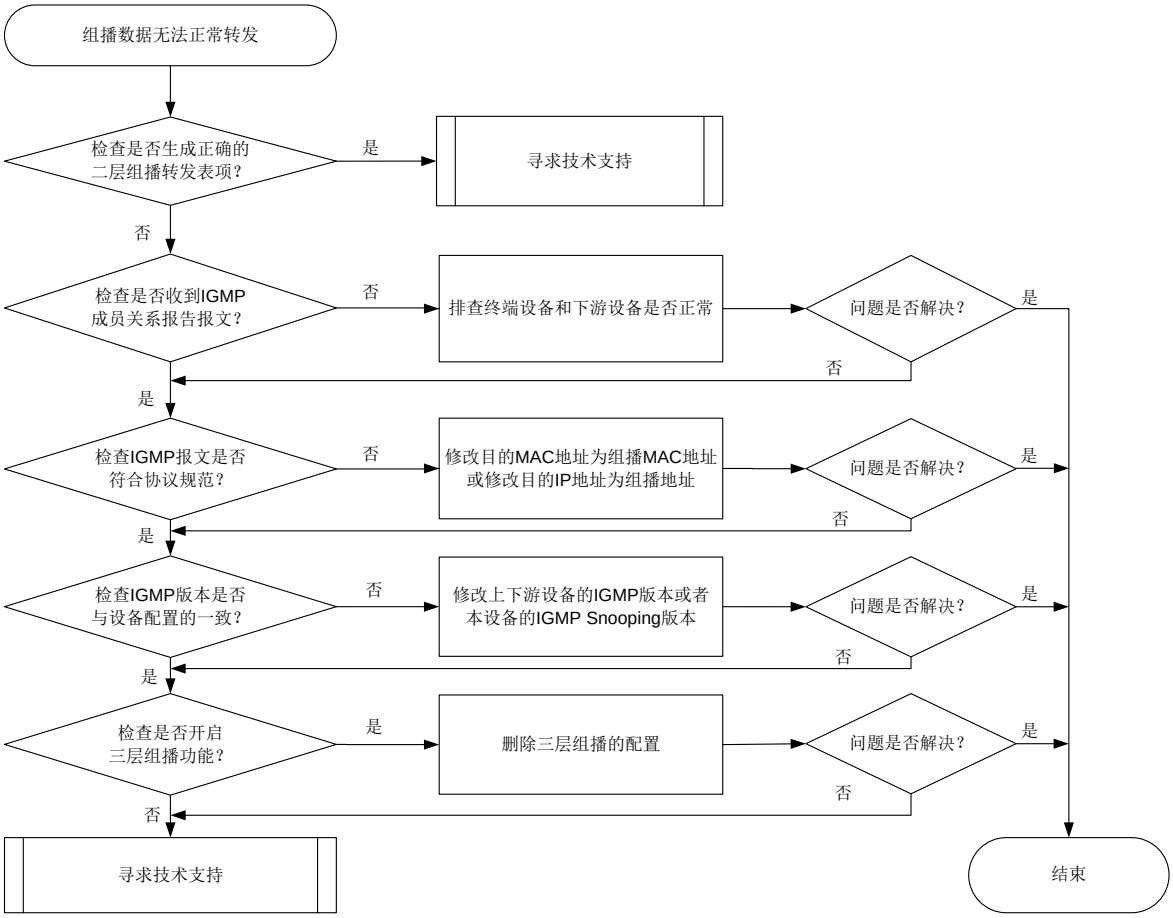
(3) 检查 IGMP 协议报文格式是否正确。

(4) 检查 IGMP 报文版本是否跟设备上配置的一致。

(5) 检查是否开启三层组播功能。

本类故障的诊断流程如图 58 所示。

图58 二层组播业务不通的故障诊断流程图



4. 处理步骤

(1) 检查是否生成正确的二层组播转发表项。

执行 **display l2-multicast ip forwarding** 命令查看二层组播表项是否生成。

- 如果存在，请直接联系技术人员。
- 如果不存在，请执行步骤(2)。

(2) 检查设备是否正常收到 IGMP 成员关系报告报文。

执行 **debugging igmp-snooping packet** 命令，打开 IGMP Snooping 报文调试信息开关。如果设备上打印如下调试信息，表示可以正常收到成员关系报告报文。

```
*Sep 15 11:47:41:455 2011 Sysname MCS/7/PACKET: -MDC=1; Receive IGMPv2 report packet
from port GE1/0/1 on VLAN 2. (G162625)
```

- 如果没有，检查下游设备和终端设备是否正常。
- 如果有，请执行步骤(3)。

(3) 检查 IGMP 协议报文交互过程是否正常，报文格式是否符合协议规范。

IGMP 协议交互不正常时，通常会出现设备上转发表项无法生成的现象，导致组播数据流无法正常转发，造成组播业务中断。

在设备上配置镜像，并联系技术支持，在专业人士的指导下使用抓包工具（例如 Wireshark）对镜像的 IGMP 协议报文进行分析。

- 如果不正常，请将 IGMP 协议报文修改为符合协议规范的报文。
- 如果正常，请执行步骤(4)。

(4) 检查收到的 IGMP 报文的版本是否与设备配置的 IGMP Snooping 版本一致。

执行 **display igmp-snooping** 命令查看显示信息中的 Version 字段确认设备使用的 IGMP Snooping 版本，检查是否与收到的 IGMP 报文的版本一致。

- 如果不一致，可以用如下两种方法处理：
  - 修改上下游设备的 IGMP 版本，保证上下游设备的 IGMP 版本与本设备上配置的 IGMP Snooping 版本一致。
  - 在本设备 IGMP-Snooping 视图下执行 **version** 命令或者在 VLAN 视图下执行 **igmp-snooping version** 命令，修改 IGMP Snooping 版本，保证本设备的 IGMP Snooping 版本与上下游设备的 IGMP 版本一致。
- 如果一致，请执行步骤(5)。

(5) 检查是否开启三层组播功能。

在开启了二层组播功能的 VLAN 所对应的 VLAN 接口上，若同时开启三层组播功能，会导致二层组播转发表项无法下发硬件，请关闭三层组播功能。

- 如果开启了三层组播功能，请删除三层组播配置。
- 如果未开启三层组播功能，请执行步骤(6)。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

10.4 三层组播故障处理

10.4.1 三层组播业务不通

1. 故障描述

三层组播业务不通主要表现在组播流量转发失败。

2. 常见原因

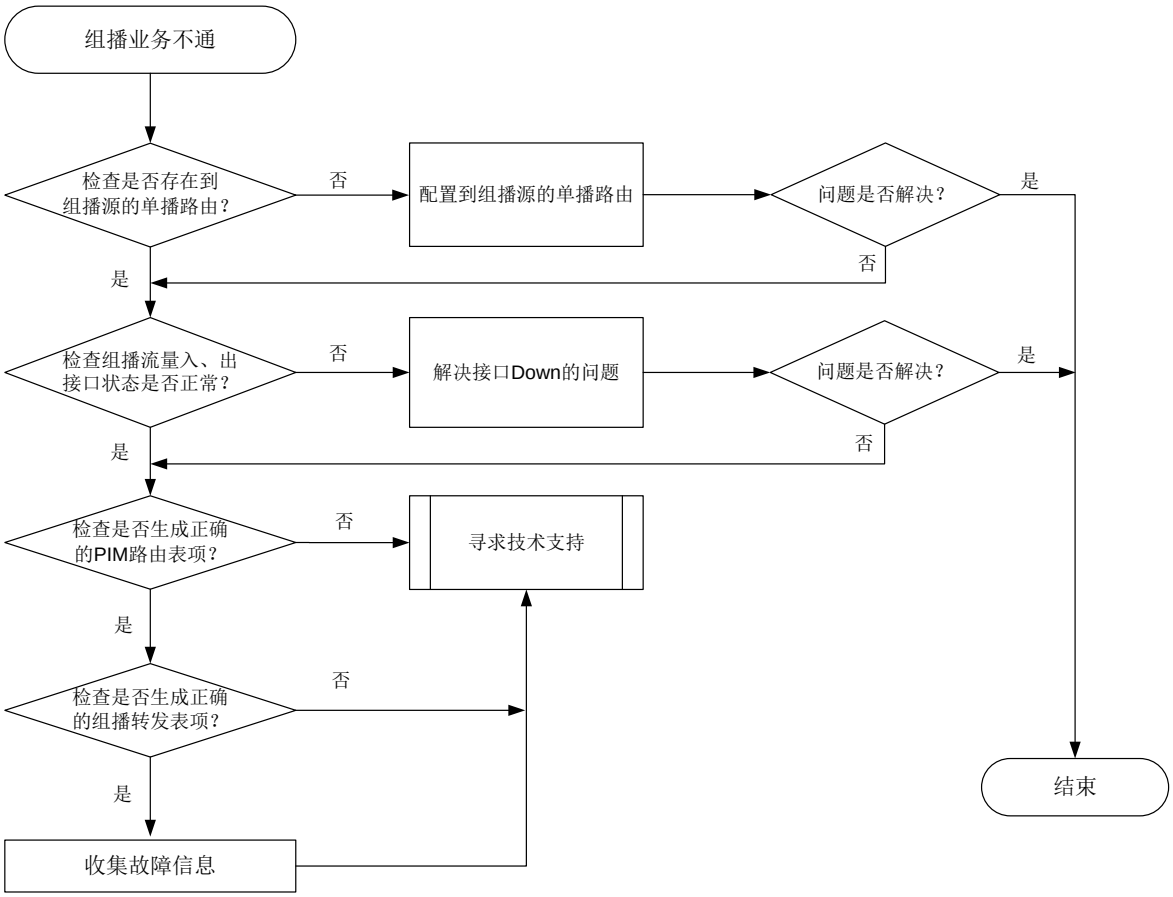
本类故障的常见原因主要包括：

- 单播路由配置错误。
- 接口状态不正确。
- PIM 路由表项未正确生成。
- 组播转发表项未正确生成。

3. 故障分析

本类故障的诊断流程如图 59 所示。

图59 三层组播业务不通的故障诊断流程图



4. 处理步骤

(1) 检查是否存在到组播源的单播路由。

执行 **display ip routing-table** *ip-address* 命令，查看是否存在到达组播源的路由。其中，*ip-address* 指定为组播源的地址。

- 如果不存在，请配置到达组播源的路由。
- 如果存在，请执行步骤(2)。

(2) 检查组播流量入、出接口的状态是否正常。

执行 **display interface** 命令查看接口物理层状态。

- 如果接口物理层状态为 Down，请解决接口故障问题。

如果接口物理层状态为 Up，请执行步骤(3)。

(3) 检查是否生成正确的 PIM 路由表项。

执行 **display pim routing-table** 命令，查看 PIM 路由表项是否生成，以及是否有对应的出接口。

- 如果没有，请联系技术支持人员。
- 如果有，请执行步骤(4)。

(4) 检查是否生成正确的组播转发表项。

执行 **display multicast forwarding-table** 命令，查看组播转发表项是否生成，以及是否有对应的出接口。

- 如果没有，请收集上述步骤的执行结果和设备的配置文件，并联系技术支持人员。
- 如果有，也请收集上述步骤的执行结果和设备的配置文件，并联系技术支持人员。

5. 告警与日志

相关告警

无

相关日志

无

10.4.2 无法正常建立 IGMP 或 MLD 表项

1. 故障描述

组播设备无法正常建立 IGMP 或者 MLD 表项。

2. 常见原因

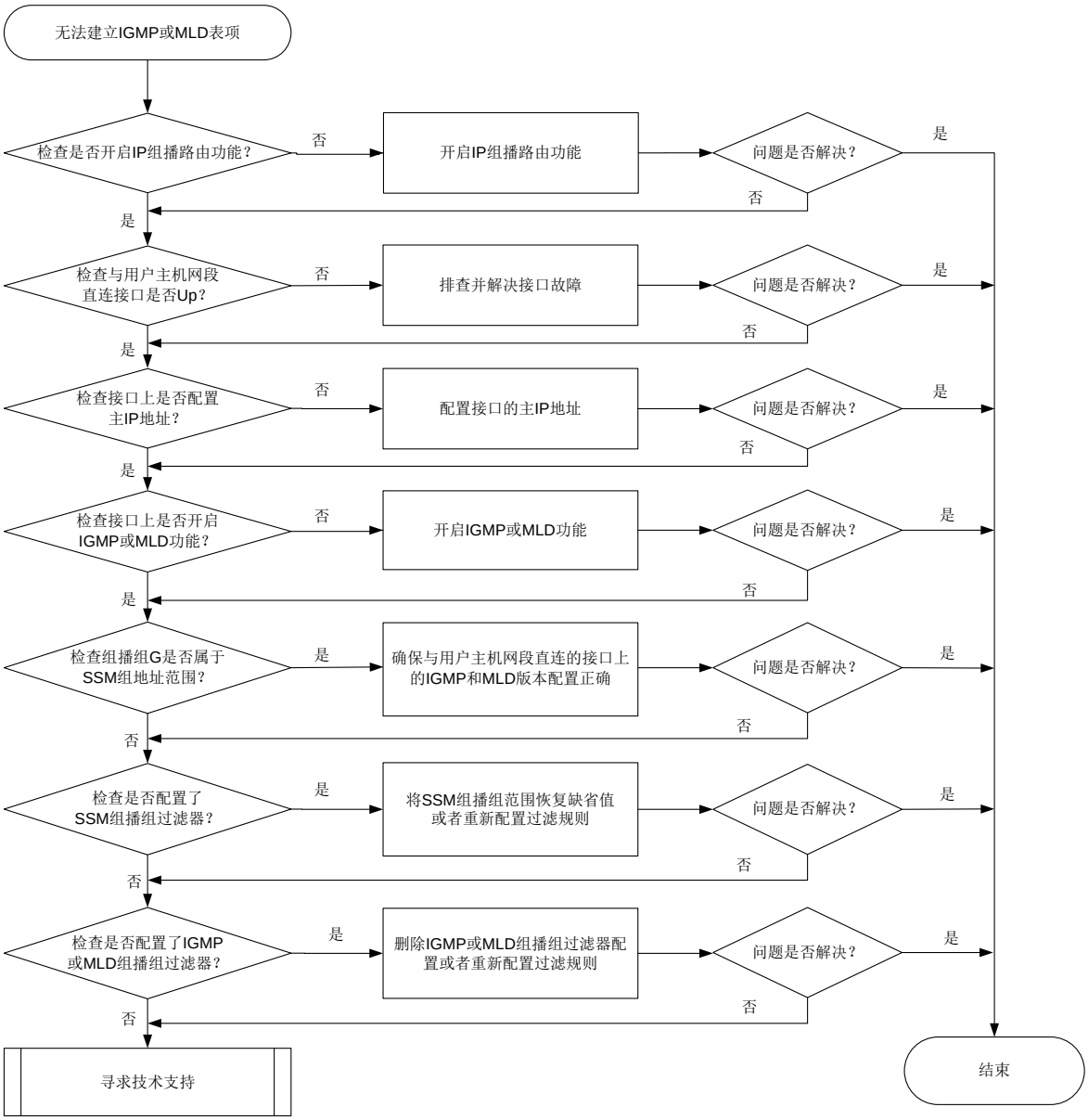
本类故障的常见原因主要包括：

- 设备上没有开启 IP 组播路由功能。
- 与用户主机网段直连的接口物理状态为 Down。
- 与用户主机网段直连的接口未配置主 IP 地址。
- 与用户主机网段直连的接口上未开启 IGMP 或 MLD 功能。
- 组播组 G 属于 SSM 组地址范围，设备上配置的 IGMP 或 MLD 版本不正确。
- 设备上配置了 SSM 组地址过滤规则，但组播组 G 地址不在 ACL 定义的 permit 规则范围内。
- 设备上配置了 IGMP 或 MLD 组播组过滤器，但组播组 G 地址不在 ACL 定义的 permit 规则范围内。

3. 故障分析

本类故障的诊断流程如图 60 所示。

图60 设备无法正常建立 IGMP 或 MLD 表项的故障诊断流程图



4. 处理步骤

(1) 检查设备上是否开启 IP 组播路由功能。

在直连用户主机网段的设备上执行 **display current-configuration | include multicast** 命令，查看是否开启 IP 组播路由功能。

- 如果未开启，请在系统视图下执行 **multicast routing** 或 **ipv6 multicast routing** 命令，开启 IP 组播路由功能。
- 如果已开启，请执行步骤(2)。

(2) 检查与用户主机网段直连接口的物理状态是否为 Up。

在直连用户主机网段的设备上执行 **display interface** *interface-type interface-number* 命令查看显示信息中的“Current state”字段，确认与用户主机网段直连的接口的物理状态是否为 Up。

a. 如果为 Up，请执行步骤(3)。

b. 如果为 Down，请排查处理接口物理 Down 的问题。

(3) 检查接口上是否配置了主 IP 地址。

在设备直连用户主机网段接口的接口视图下执行 **display this** 命令，查看是否通过 **ip address** 命令配置了接口的主 IP 地址。

a. 如果没有配置，请在接口上通过 **ip address** 命令进行配置。

b. 如果已配置，请执行步骤(4)。

(4) 检查与用户主机网段直连接口上是否开启 IGMP 或 MLD 功能。

在直连用户主机网段的设备上执行 **display current-configuration interface** 命令，查看与用户主机网段直连的接口上是否开启 IGMP 或 MLD 功能。

a. 如果没有开启，请在相应的接口上开启 IGMP 或 MLD 功能。

b. 如果已开启，请执行步骤(5)。

(5) 检查组播组 G 是否属于 SSM 组地址范围。

- 对于 IGMP 表项无法生成的情况：

  请检查组播组 G 是否属于 SSM 组地址范围，SSM 组播组地址的范围为 232.0.0.0/8。

  - 如果属于，请确保与用户主机网段直连的接口上的 IGMP 版本为 IGMPv3，并确认 IGMPv3 的报文正确。如果故障仍未排除，请执行步骤(6)。
  - 如果不属于，请执行步骤(7)。

- 对于 MLD 表项无法生成的情况：

  请检查组播组 G 是否属于 IPv6 SSM 组地址范围，IPv6 SSM 组播组的范围为 FF3x::/32。

  - 如果属于，请确保与用户主机网段直连的接口上的 MLD 版本为 MLDv2。如果故障仍未排除，请执行步骤(6)。
  - 如果不属于，请执行步骤(7)。

(6) 检查是否配置了 SSM 组播组过滤器。

在直连用户主机网段的设备上执行 **display current-configuration configuration pim** 或者 **display current-configuration configuration pim6** 命令，查看是否已通过 **ssm-policy** 命令配置 SSM 组播组的范围。

- 如果已配置，请检查组播组 G 是否在 ACL 规则允许的范围之内。
  - 如果不在，建议根据实际组网在 PIM 视图下执行 **undo ssm-policy** 命令恢复缺省情况；重新配置 ACL 规则，使得组播组 G 地址在 ACL 的 permit 规则中。
  - 如果在，请执行步骤(7)。
- 如果未配置，请执行步骤(7)。

(7) 检查接口上是否配置了 IGMP 或 MLD 组播组过滤器。

在直连用户主机网段的设备上执行 **display current-configuration** 命令，查看是否已通过 **igmp group-policy** 或 **mld group-policy** 命令配置了 IGMP 或 MLD 组播组过滤器。

- 如果已配置，请检查组播组 G 是否在 ACL 规则允许的范围之内。
  - 如果不在，建议根据实际组网需要执行 **undo igmp group-policy** 或 **undo mld group-policy** 命令删除该组播组过滤器配置；重新配置 ACL 规则，使得组播组 G 地址在 ACL 的 permit 规则中。
  - 如果在，请执行步骤(8)。

- 如果未配置，请执行步骤(8)。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11 MPLS 类故障处理

11.1 LDP故障处理

11.1.1 LDP 会话无法 Up

1. 故障描述

LDP 会话无法 Up。

2. 常见原因

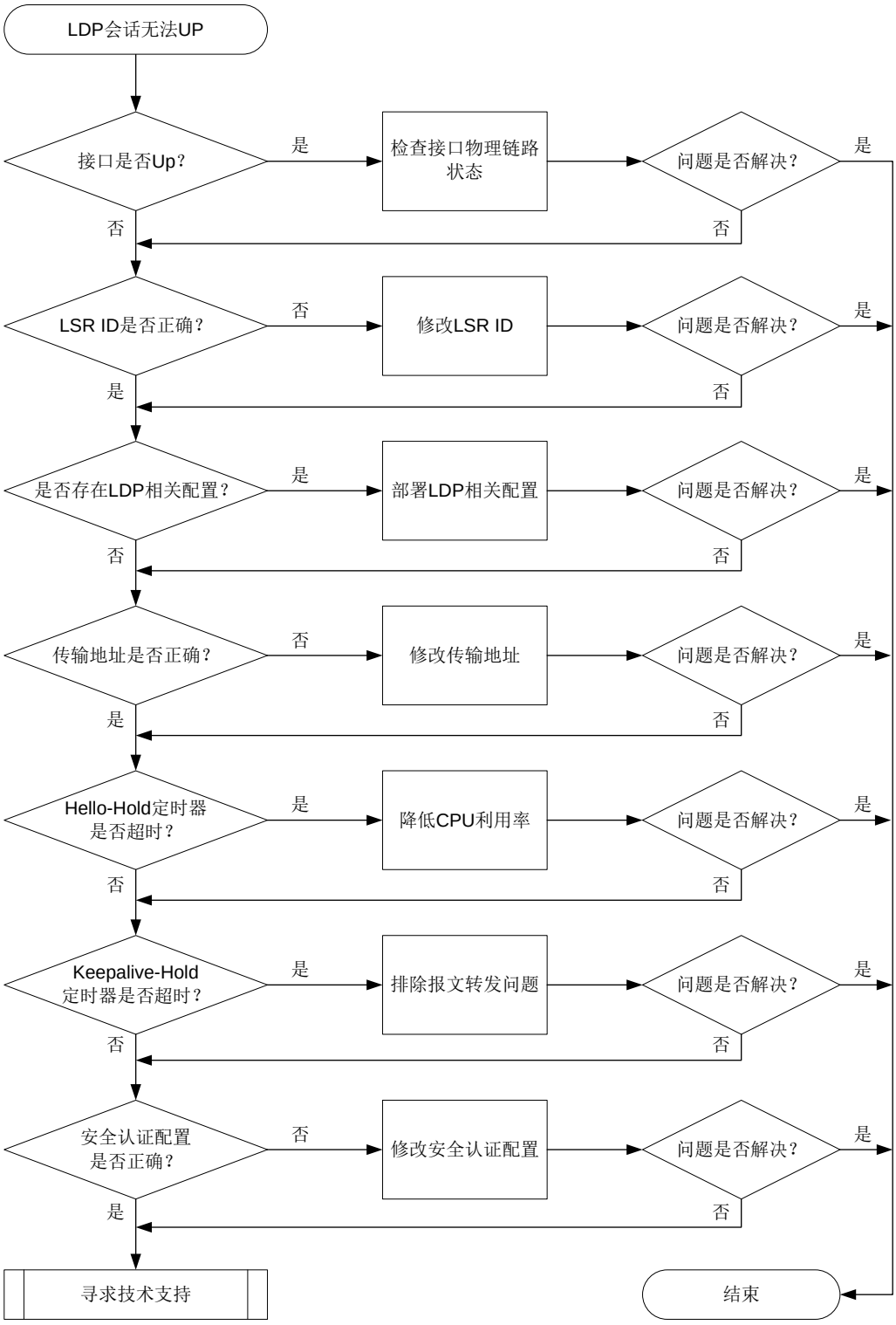
本类故障的常见原因主要包括：

- 建立会话的接口处于 Down 状态
- LSR ID 配置错误
- 不存在 LDP 会话的相关配置
- 传输地址配置错误
- LDP Hello-hold 定时器超时
- LDP Keepalive-hold 定时器超时
- 安全认证配置错误

3. 故障分析

本类故障的诊断流程如图 61 所示。

图61 LDP 会话 Down 的故障诊断流程图



4. 处理步骤

(1) 检查建立 LDP 会话的接口是否处于 Up 状态。

执行 **display interface** 命令查看接口是否处于 UP 状态：

- 如果没有 UP，则排除接口物理链路故障，使接口处于 UP 状态。
- 如果接口处于 UP 状态，则执行步骤(2)。

(2) 检查 LSR ID 配置是否正确。

LSR ID 包括 Local LSR ID、LDP LSR ID 和 MPLS LSR ID。LSR ID 优先级从高到底依次为 Local LSR ID、LDP LSR ID、MPLS LSR ID。设备上至少配置其中的一种 LSR ID，且该 LSR ID 必须路由可达。

执行 **display mpls ldp peer verbose** 命令检查是否配置了 LSR ID：

```
<Sysname> display mpls ldp peer verbose
VPN instance: public instance
 Peer LDP ID      : 100.100.100.20:0
 Local LDP ID     : 100.100.100.17:0
 TCP Connection   : 100.100.100.20:47515 -> 100.100.100.17:646
…
```

如果至少配置了一种 LSR ID，则执行步骤(3)。

(3) 检查是否存在 LDP 会话的相关配置。

如果是直连会话，则在接口视图下执行 **display this** 命令，查看是否存在 LDP 会话的相关配置。

a. 如果配置信息中没有包含 **mpls enable** 命令、**mpls ldp enable** 命令、**mpls ldp ipv6 enable** 命令或 **mpls ldp transport-address** 命令，则部署对应的配置。

b. 如果存在 LDP 会话的相关配置，则执行步骤(4)。

如果是 LDP 远程会话，则在 LDP 视图下执行 **display this** 命令，查看是否存在 LDP 会话的相关配置。

c. 如果配置信息中没有包含 **targeted-peer** 或 **mpls ldp transport-address** 命令，则部署对应的配置。

d. 如果存在 LDP 会话的相关配置，则执行步骤(4)。

(4) 检查传输地址配置是否正确。

如果是 LDP IPv4 会话，请执行 **display mpls ldp discovery verbose** 命令检查传输地址配置是否正确：

```
<Sysname> display mpls ldp discovery verbose
VPN instance: public instance
Link Hellos:
  Interface GigabitEthernet1/0/2
    Local LDP ID     : 100.100.100.17:0
    Hello Interval   : 5000 ms            Hello Sent/Rcvd  : 83/160
    Transport Address: 100.100.100.17
    Peer LDP ID      : 100.100.100.18:0
      Source Address : 202.118.224.18     Transport Address: 100.100.100.18
      Hello Hold Time: 15 sec (Local: 15 sec, Peer: 15 sec)
    Peer LDP ID      : 100.100.100.20:0
      Source Address : 202.118.224.20     Transport Address: 100.100.100.20
      Hello Hold Time: 15 sec (Local: 15 sec, Peer: 15 sec)

Targeted Hellos:
  100.100.100.17 -> 100.100.100.18 (Active, Passive)
```

```
    Local LDP ID     : 100.100.100.17:0
    Hello Interval   : 15000 ms           Hello Sent/Rcvd  : 23/20
    Transport Address: 100.100.100.17
    Session Setup    : Config/Tunnel
    Peer LDP ID      : 100.100.100.18:0
      Source Address : 100.100.100.18     Transport Address: 100.100.100.18
      Hello Hold Time: 45 sec (Local: 45 sec, Peer: 45 sec)
```

如果是 LDP IPv6 会话，请执行 **display mpls ldp discovery ipv6 verbose** 命令检查传输地址配置是否正确：

```
<Sysname> display mpls ldp discovery ipv6 verbose
VPN instance: public instance
Link Hellos:
  Interface GigabitEthernet1/0/2
    Hello Interval   : 5000 ms            Hello Sent/Rcvd  : 83/160
    Transport Address: 2001::2
    Peer LDP ID      : 100.100.100.18:0
      Source Address : FE80:130F:20C0:29FF:FEED:9E60:876A:130B
      Transport Address: 2001::1
      Hello Hold Time: 15 sec (Local: 15 sec, Peer: 15 sec)

Targeted Hellos:
  2001:0000:130F::09C0:876A:130B ->
        2005:130F::09C0:876A:130B(Active, Passive)
    Hello Interval   : 15000 ms           Hello Sent/Rcvd  : 23/22
    Transport Address: 2001:0000:130F::09C0:876A:130B
    Peer LDP ID      : 100.100.100.18:0
      Source Address : 2005:130F::09C0:876A:130B
      Destination Address : 2001:0000:130F::09C0:876A:130B
      Transport Address   : 2005:130F::09C0:876A:130B
      Hello Hold Time: 45 sec (Local: 45 sec, Peer: 45 sec)
```

如果传输地址配置不正确，则可以在接口视图或 LDP 对等体视图下执行 **mpls ldp transport-address** 命令配置传输地址。缺省情况下，传输地址为本 LSR 的 LSR ID。

如果传输地址配置正确，则需要确认路由是否发布。执行 **display ip routing-table** 命令，查看是否存在到达会话对端的路由。

a. 如果不存在到达会话对端的路由，则请将传输地址配置成本机存在的 IP 地址，确保路由正确发布。

b. 如果存在到达会话对端的路由，则执行步骤(5)。

(5) 检查 LDP Hello-hold 定时器是否超时。

建议每 5 秒执行一次 **display mpls ldp discovery** 命令，查看收发 Hello 消息的计数，检查会话两端的 Hello 消息是否都正常发送。若连续几次执行命令后发现发送或接收的计数没有变化，则表示 Hello 消息收发异常，Hello-hold 定时器超时。

- 如果 Hello-hold 定时器超时，请排除链路问题，并检查设备 CPU 利用率。如果 CPU 利用率过高，请关闭一些不必要功能；如果 CPU 利用率正常，则执行步骤(6)。
- 如果 Hello-hold 定时器没有超时，则执行步骤(6)。

(6) 检查 LDP Keepalive-hold 定时器是否超时。

建议每 15 秒执行一次 **display mpls ldp peer** 命令，查看收发的 Keepalive 消息的计数，检查会话两端的 Keepalive 消息是否都正常发送。若连续几次执行命令后发现发送或接收的计数没有变化，则表示 Keepalive 消息收发异常，Keepalive-hold 定时器超时。

- 如果 Keepalive-hold 定时器超时，则排除报文转发问题。
- 如果 Keepalive-hold 定时器没有超时，则执行步骤(7)。

(7) 安全认证配置是否正确。

请执行 **display mpls ldp peer** 命令 LDP 会话之间的安全认证是否配置，以及配置的安全认证类型是否一致：

```
<Sysname> display mpls ldp peer
VPN instance: public instance
Total number of peers: 1
Peer LDP ID            State         Role     GR   Auth      KA Sent/Rcvd
2.2.2.9:0              Operational   Passive  Off  Keychain  39/39
```

- 如果 LDP 会话两端 Auth 字段显示不一致，则将 LDP 会话两端的安全认证修改为一致。
- 如果 LDP 会话两端 Auth 字段显示一致，则执行步骤(8)。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：MPLS-LDP-STD-MIB

- mplsLdpSessionDown (1.3.6.1.2.1.10.166.4.0.4)

相关日志

- LDP/4/LDP_SESSION_CHG

11.1.2 LDP 会话震荡

1. 故障描述

LDP 会话状态频繁震荡。

2. 常见原因

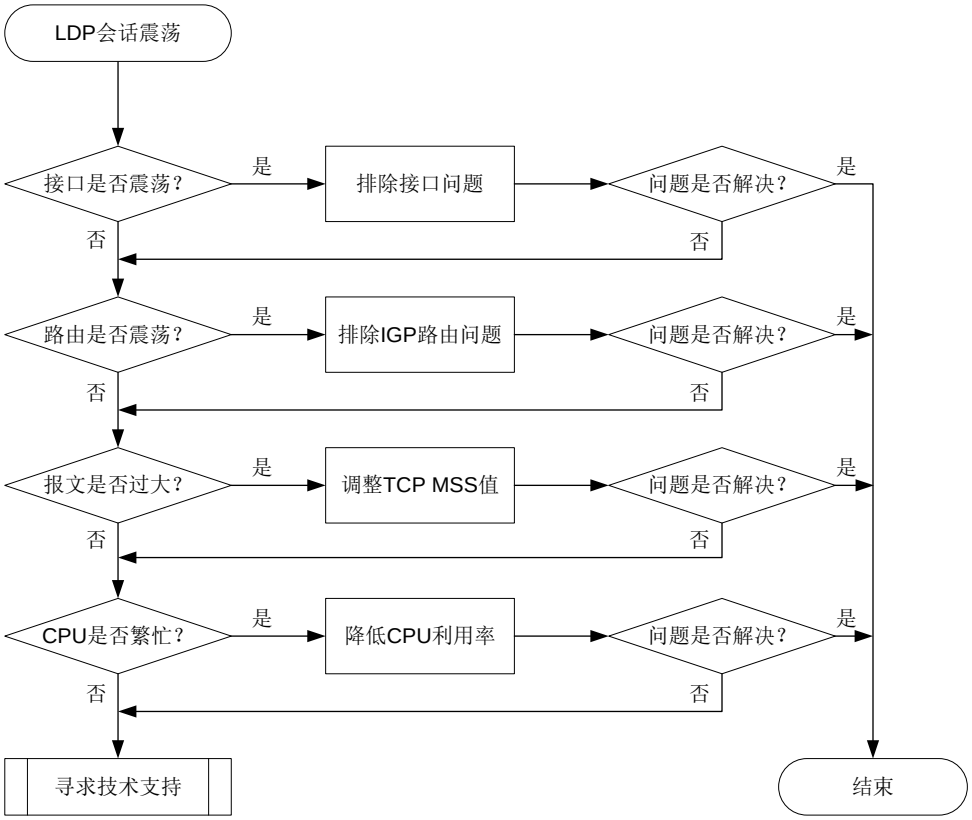
本类故障的常见原因主要包括：

- 接口震荡
- 路由震荡
- CPU 利用率过高

3. 故障分析

本类故障的诊断流程如图 62 所示。

图62 LDP 会话震荡的故障诊断流程图



4. 处理步骤

(1) 检查接口是否震荡。

执行 **display interface brief** 命令，查看 Physical 和 Protocol 字段。Physical 和 Protocol 字段均显示 Up，则表示接口状态为 Up，否则表示接口状态为 Down。若接口一直在 Up 和 Down 两种状态间切换，则表示接口震荡。

- 如果接口震荡，则排除接口问题。
- 如果接口没有震荡，请执行步骤(2)。

(2) 检查路由是否震荡。

执行 **display ip routing-table** 命令，查看路由信息。如果路由信息一直在显示和不显示两种情况切换，则表示路由震荡。

- 如果路由震荡，或者路由一直不存在，则排除链路问题和排除 IGP 路由问题。
- 如果路由没有震荡，则执行步骤(3)。

(3) TCP 报文是否过大。

执行 **display tcp statistics** 命令，查看 TCP 连接的流量统计信息。通过 Sent packets 信息中 data packets retransmitted（重发的数据报文数）字段的值，判断 TCP 报文是否过大：

- 如果重发的数据报文数不断增加，则表示 TCP 报文过大，请在报文出接口下执行 **tcp mss** 命令调整 TCP MSS 值。
- 如果重发的数据报文数未增加，则表示 TCP 报文大小正常，请执行步骤(4)。

(4) 检查 CPU 利用率是否过高。

执行 **display cpu-usage** 命令，查看 CPU 利用率的统计信息。

- 如果 CPU 利用率过高，则关闭一些不必要的功能，降低设备 CPU 利用率。
- 如果 CPU 利用率正常，则执行步骤(5)。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：MPLS-LDP-STD-MIB

- mplsLdpSessionDown (1.3.6.1.2.1.10.166.4.0.4)

相关日志

- LDP/4/LDP_SESSION_CHG

11.1.3 LDP LSP 无法 Up

1. 故障描述

LDP 网络中 LDP LSP 无法 Up。

2. 常见原因

本类故障的常见原因主要包括：

- 路由问题
- LDP 会话 Down
- 资源不足，如 Label 达到上限，内存不足等
- 配置了 LSP 触发策略、标签接受控制策略、标签通告控制策略或 Label Mapping 消息的发送策略
- 路由的出接口与 LDP 建立会话的接口不一致

3. 故障分析

本类故障的诊断思路如下：

(1) 检查路由是否存在。

(2) 检查 LDP 会话是否正常建立。

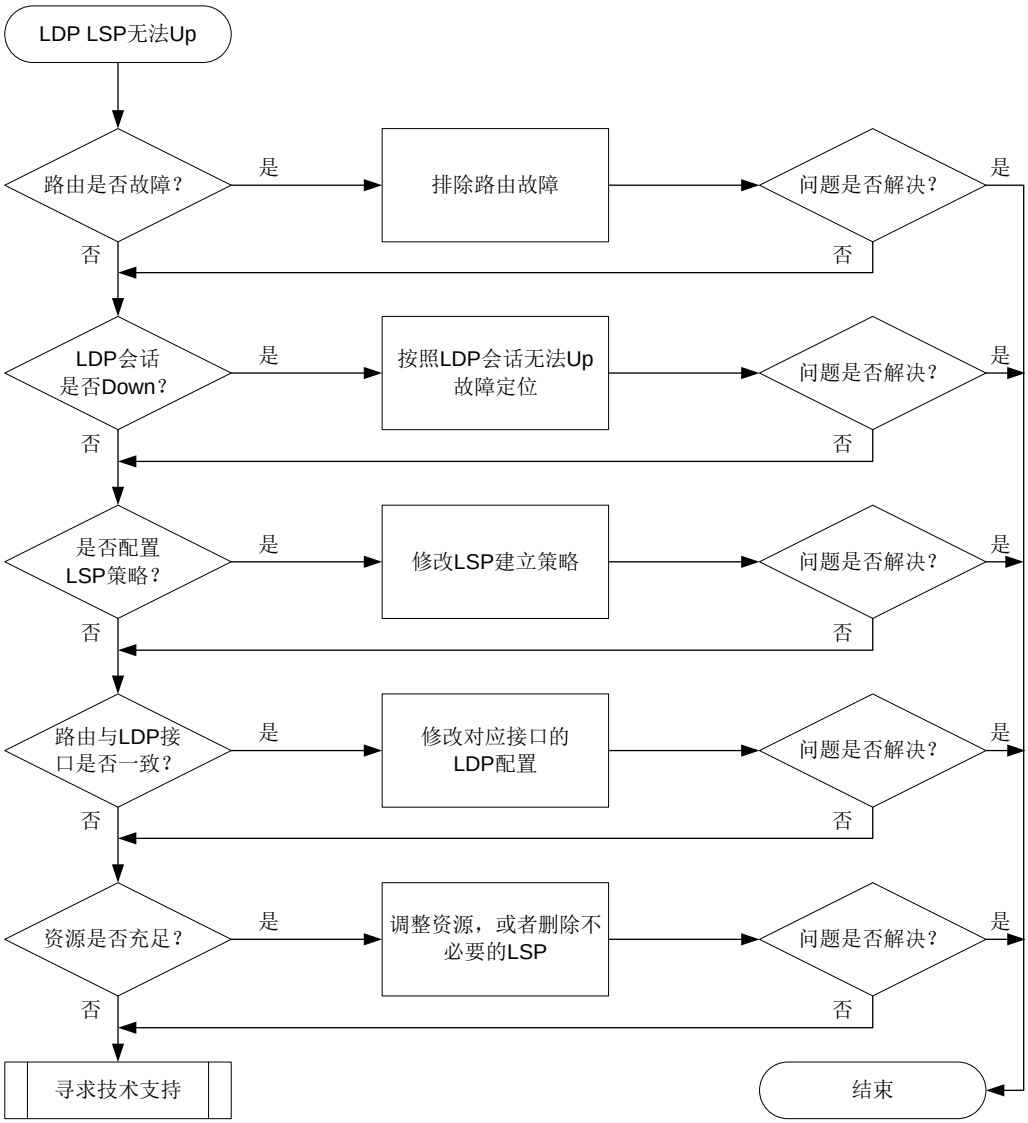
(3) 检查是否存在资源不足，入 Label 达到上限，内存不足的问题。

(4) 检查是否配置了 LSP 建立策略。

(5) 检查路由的出接口与 LDP 建立会话的接口是否一致。

本类故障的诊断流程如图 63 所示。

图63 LDP LSP Down 的故障诊断流程图



4. 处理步骤

(1) 检查路由是否存在。

执行 **display ip routing-table** *ip-address mask* **verbose** 命令，查看是否存在到达指定 LSP 目的地址的路由，并检查该路由是否处于激活状态（路由信息中的 State 字段为 Active Adv，表示路由处于激活状态）。对于公网 BGP 路由，还需要检查路由是否带标签。如果 Label 字段非 NULL，则表示 BGP 路由携带标签。路由存在时，会显示相关路由信息。路由不存在时，则不会显示相关路由信息。

```
<Sysname> display ip routing-table 1.1.1.1 32 verbose

Summary count : 1

 Destination: 1.1.1.1/32
    Protocol: O_INTRA
  Process ID: 1
```

```
   SubProtID: 0x1                    Age: 00h00m16s
  FlushedAge: 00h00m16s
        Cost: 1                 Preference: 10
       IpPre: N/A               QosLocalID: N/A
         Tag: 0                      State: Active Adv
   OrigTblID: 0x0                OrigVrf: default-vrf
```

…

- 如果路由不存在、路由存在但未处于激活状态或者 BGP 路由未携带标签，则请排除路由故障。
- 如果路由存在且处于激活状态，对于 BGP 路由也带标签，则执行步骤(2)。

(2) 检查 LDP 会话是否正常建立。

执行 **display mpls ldp peer verbose** 命令，查看 LDP 会话是否成功建立：

```
<Sysname> display mpls ldp peer verbose
VPN instance: public instance
 Peer LDP ID      : 1.1.1.1:0
 Local LDP ID     : 2.2.2.2:0
 TCP Connection   : 2.2.2.2:14080 -> 1.1.1.1:646
 Session State    : Operational       Session Role     : Active
 Session Up Time  : 0000:00:14 (DD:HH:MM)
```

…

- 如果State字段显示不是Operational，则表示LDP会话没有正常建立，请参见“11.1.1 LDP会话无法 Up”故障进行定位。
- 如果 State 字段的显示为 Operational，则表示 LDP 会话已建立并处于 Up 状态，请执行步骤(3)。

(3) 检查是否配置了 LSP 策略。

- 在 LDP 视图下执行 **display this** 命令，如果存在以下命令，则需要检查 IP 前缀列表是否过滤了指定的 LSP：
  - **lsp-trigger prefix-list**
  - **accept-label peer prefix-list**
  - **advertise-label prefix-list**
  - **propagate mapping prefix-list**

  如果 IP 前缀列表过滤了指定的 LSP，则请修改 IP 前缀列表，使其允许指定 LSP 目的地址通过；如果 IP 前缀列表没有过滤指定的 LSP，则执行步骤(4)。
- 如果 LDP 视图下没有配置以上命令，则执行步骤(4)。

(4) 检查路由的出接口与 LDP 建立会话的接口是否一致。

执行 **display ip routing-table** *ip-address mask* 命令，查看指定路由的出接口信息：

```
<Sysname> display ip routing-table 1.1.1.1 32

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
1.1.1.1/32          O_INTRA 10  1           10.1.1.1        GE1/0/1
```

执行 **display mpls ldp peer** *peer-lsr-id* **verbose** 命令，查看指定 LDP 对等体的 Discovery Sources 信息：

```
<Sysname> display mpls ldp peer 1.1.1.1 verbose
VPN instance: public instance
 Peer LDP ID      : 1.1.1.1:0
 Local LDP ID     : 2.2.2.2:0
 TCP Connection   : 2.2.2.2:14080 -> 1.1.1.1:646
 Session State    : Operational        Session Role     : Active
 Session Up Time  : 0000:00:55 (DD:HH:MM)
 Max PDU Length   : 4096 bytes (Local: 4096 bytes, Peer: 4096 bytes)
 Keepalive Time     : 45 sec (Local: 45 sec, Peer: 45 sec)
 Keepalive Interval : 15 sec
 Msgs Sent/Rcvd   : 229/228
 KA Sent/Rcvd     : 223/223
 Label Adv Mode   : DU                 Graceful Restart : Off
 Reconnect Time   : 0 sec              Recovery Time    : 0 sec
 Loop Detection   : Off                Path Vector Limit: 0
 mLDP P2MP        : Off
 Discovery Sources:
   GigabitEthernet1/0/1
     Hello Hold Time: 15 sec           Hello Interval   : 5000 ms
 Addresses received from peer:
   10.1.1.1          1.1.1.1
```

- 如果 Discovery Sources 信息的接口信息不包含指定路由的出接口，则检查指定路由的出接口上对应的 LDP 配置是否正确，及下游设备对应接口的 LDP 配置是否正确。如果不正确，则修改相应配置；如果正确，则执行步骤(5)
- 如果 Discovery Sources 信息的接口信息包含指定路由的出接口，则执行步骤(5)。

(5) 检查是否资源不足，如内存不足，LSP 数量达到上限的问题。

- 检查系统内存是否不足

  执行 **display memory-threshold** 命令，查看系统内存是否不足。如果存在内存不足，则删除不必要的 LSP。

- 检查标签数量是否超出上限。

  执行 **display mpls summary** 命令，查看 LDP 的标签段剩余标签数量是否为 0，即 Idle 字段显示为 0。如果 LDP 标签段剩余标签数量为 0，则表示 LDP 的标签资源全部使用完，需要删除不必要的 LSP。

```
<Sysname> display mpls summary
MPLS LSR ID      : 2.2.2.2
Egress Label Type: Implicit-null
Entropy Label    : Off
Labels:
  Range                              Used/Idle/Total         Owner
  16-2047                            0/2032/2032             StaticPW
                                                             Static
                                                             StaticCR
                                                             Static SR Adj
                                                             BSID
```

```
2048-599999                    9129/588823/597952    LDP
                                                     RSVP
                                                     BGP
                                                     BGP SR EPE
                                                     OSPF SR Adj
                                                     ISIS SR Adj
```

- 如果不存在资源不足问题，请执行步骤(6)。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：MPLS-LSR-STD-MIB

- 节点名称 (OID) mplsXCDown (1.3.6.1.2.1.10.166.2.0.2)

相关日志

无

11.1.4 LDP LSP 震荡

1. 故障描述

LDP 网络中 LDP LSP 频繁震荡。

2. 常见原因

本类故障的常见原因主要包括：

- 路由震荡。
- LDP 会话震荡。

3. 故障分析

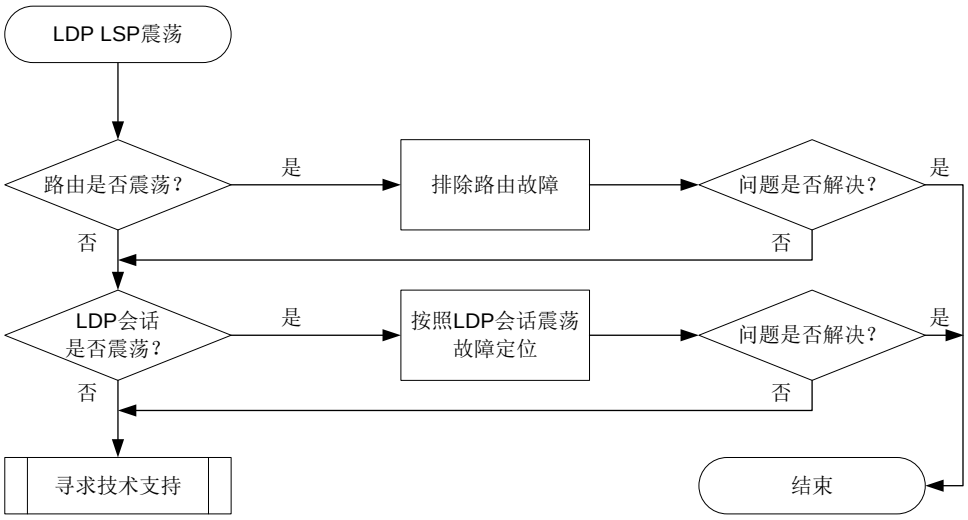
本类故障的诊断思路如下：

(1) 检查路由是否震荡。

(2) 检查 LDP 会话是否震荡。

本类故障的诊断流程如图 64 所示。

图64 LDP LSP 震荡的故障诊断流程图



4. 处理步骤

(1) 检查路由是否震荡。

建议每 1 秒执行一次 **display ip routing-table** 命令，连续执行 5～10 次，查看到达 LSP 目的地址的路由信息。路由存在时，会显示相关路由信息。路由不存在时，则不会显示相关路由信息。如果相关路由信息一直在显示和不显示两种情况切换，则表示路由震荡。

查看路由信息后，请执行 **display mpls ldp fec** 命令查看 LSP 下游信息，即 Downstream Info 中的 State 字段，确保与下游对等体建立的 LSP 处于激活状态（Established）。

```
<Sysname> display mpls ldp fec
VPN instance: public instance
 FEC: 1.1.1.1/32
   Flags: 0x112
   In Label: 2175
   Upstream Info:
     Peer: 1.1.1.1:0                State: Established
   Downstream Info:
     Peer: 1.1.1.1:0
       Out Label: 3                 State: Established
       Next Hops: 10.1.1.1                 GE1/0/1
   RIB Info:
     Protocol        : OSPF         BGP As Num   : 0
     Label Proto ID  : 1            NextHopCount : 1
     VN ID           : 0x313000003
     Tunnel ID       : -
```

- 如果路由震荡，或者路由一直都不存在，则请排除路由问题。
- 如果路由没有震荡，则执行步骤(2)。

(2) 检查 LDP 会话是否震荡。

建议每 1 秒执行一次 **display mpls ldp peer** 命令，连续执行 5～10 次，查看显示信息的 State 字段。如果该字段的取值在 Operational 状态和其他非 Operational 状态之间切换，则表示 LDP 会话震荡。

```
<Sysname> display mpls ldp peer
VPN instance: public instance
Total number of peers: 1
Peer LDP ID            State         Role     GR   AUT       KA Sent/Rcvd
1.1.1.1:0              Operational   Active   Off  None      298/298
```

- 如果 LDP 会话震荡，则请参见“11.1.2 LDP 会话震荡”故障进行定位。
- 如果 LDP 会话没有震荡，则执行步骤(3)。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：MPLS-LSR-STD-MIB

- 节点名称 (OID) mplsXCDown (1.3.6.1.2.1.10.166.2.0.2)

相关日志

无

11.2 MPLS L2VPN/VPLS故障处理

11.2.1 PW ping 不通

1. 故障描述

执行 **ping mpls pw** 命令检测 PW 连通性，发现 ping 不通对端。

2. 常见原因

本类故障的常见原因主要包括：

- 检测的 PW 不存在。
- PW 模板配置错误。
- PW 故障。
- PW 不存在有效的公网转发路径。

3. 故障分析

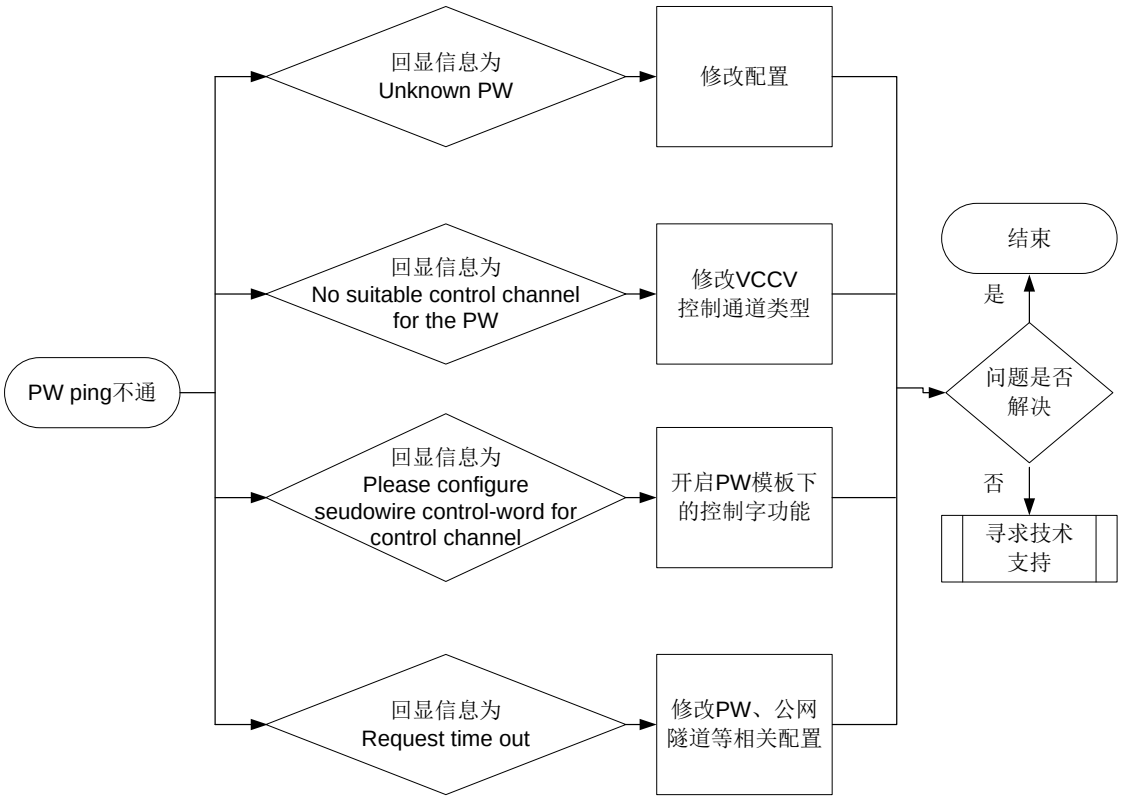
本类故障需要根据 **ping mpls pw** 命令的回显信息进行分析和定位，具体诊断思路如下：

- 回显信息为 Unknown PW 时，表示检测的 PW 不存在，需要修改配置来解决本类故障。
- 回显信息为 No suitable control channel for the PW 时，表示 PW 的 VCCV 控制通道类型配置错误，需要通过 **vccv cc** 命令修改 PW 模板中 VCCV 控制通道类型来解决本类故障。
- 回显信息为 Please configure pseudowire control-word for control channel 时，表示 PW 引用的 PW 模板中未开启控制字功能，需要通过 **control-word enable** 命令在 PW 模板下开启控制字功能来解决本类故障。

- 回显信息为 Request time out 时，先排查本端 PW 是否 Up，再通过 **tracert mpls pw** 命令来定位故障节点。

本类故障的诊断流程如图 65 所示。

图65 PW ping 不通的故障诊断流程图



4. 处理步骤

回显信息为 Unknown PW 时，本类故障的处理步骤为：修改配置确保检测的 PW 存在。

回显信息为 No suitable control channel for the PW 时，本类故障的处理步骤为：通过 **vccv cc** 命令将 PW 两端的 VCCV 控制通道类型配置一致。

回显信息为 Please configure pseudowire control-word for control channel 时，本类故障的处理步骤为：通过 **control-word enable** 命令在 PW 模板下开启控制字功能。

回显信息为 Request time out 时，本类故障的处理步骤如下：

(1) 执行 **display l2vpn pw** 命令查看 PW 是否 Up。

```
<Sysname> display l2vpn pw
Flags: M - main, B - backup, E - ecmp, BY - bypass, H - hub link, S - spoke link
       N - no split horizon, A - administration, ABY - ac-bypass
       PBY - pw-bypass
Total number of PWs: 2
2 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

Xconnect-group Name: ldp
Peer            PWID/RmtSite/SrvID In/Out Label   Proto  Flag Link ID  State
192.3.3.3       500                1299/1299      LDP    M    0        Up
```

```
VSI Name: aaa
Peer            PWID/RmtSite/SrvID In/Out Label   Proto  Flag Link ID  State
2.2.2.9         2                  1420/1419      BGP    M    9        Up
```

- 若 PW 为 Down 状态，请通过 **display l2vpn pw verbose** 命令查看 PW 状态变为 Down 的原因，并根据故障原因进行故障处理。

```
<Sysname> display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          Remote Site: 2
    Signaling Protocol  : BGP
    Link ID             : 9          PW State : Down
    In Label            : 1420       Out Label: 1419
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Flow Label          : Send
    Control Word        : Disabled
    Tunnel Group ID     : 0x8000009600000000
    Tunnel NHLFE IDs    : 1038
    Admin PW            : -
    E-Tree Mode         : -
    E-Tree Role         : root
    Root VLAN           : -
    Leaf VLAN           : -
    Down Reasons        : Control word not match
```

常见的故障原因及处理方法如下：

- BFD session for PW down：用来检测 PW 的 BFD 会话状态为 down，此类故障的处理方式为，通过 **display bfd session** 命令查看 BFD 状态为 down 的原因，检查并修改 BFD 配置或检查物理链路是否存在链路故障、链路质量问题。
- BGP RD was deleted：BGP 的 RD 被删除，此类故障的处理方式为，在交叉连接组自动发现视图下配置 **route-distinguisher** *route-distinguisher* 命令。
- BGP RD was empty：未配置 BGP 的 RD，此类故障的处理方式为，在交叉连接组自动发现视图下配置 **route-distinguisher** *route-distinguisher* 命令。
- Control word not match：PW 两端控制字功能配置不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的控制字功能（通过 **control-word enable** 命令开启）配置一致。
- Encapsulation not match：PW 两端封装类型不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的 PW 数据封装类型（通过 **pw-type** 命令配置）配置一致。
- LDP interface parameter not match：PW 两端接口 LDP 协商参数不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的 VCCV 控制通道类型（通过 **vccv cc** 命令配置）配置一致或将 PW 两端关联的电路仿真接口下引用的电路仿真类中的配置保持一致。
- Non-existent remote LDP PW：对端设备已删除 LDP PW，此类故障的处理方式为，在对端设备上重新配置 PW。

- Local AC Down：本地 AC 状态为 down，此类故障的处理方式为，检查并修改 AC 接口上的配置或排除 AC 所在的接口的故障，保障接口为 Up 状态。
- Local AC was non-existent：未配置本地 AC，此类故障的处理方式为，配置本地的 AC 并关联 VSI。
- MTU not match：PW 两端 MTU 不一致，此类故障的处理方式为，将 PW 两端的 MTU 配置一致或者通过 **mtu-negotiate disable** 命令关闭 PW MTU 协商功能。
- Remote AC Down：对端 AC 状态 down，此类故障的处理方式为，检查并修改对端 AC 接口上的配置或排除 AC 所在的接口的故障，保障接口为 Up 状态。

○ 若 PW 为 Up 状态，请继续执行第(2)步。

(2) 执行 **display l2vpn forwarding pw verbose** 命令，查看 PW 的转发信息中入标签（In Label）、出标签（Out Label）和承载 PW 的隧道对应的 NHLFE 表项索引值（Tunnel NHLFE IDs）是否为有效值。

```
<Sysname> display l2vpn forwarding pw verbose
Xconnect-group Name: xcg1
 Connection Name: c1
  Link ID: 0
    PW Type           : VLAN                  PW State : Up
    In Label          : 110126                Out Label: 130126
    MTU               : 1500
    PW Attributes     : Main
    VCCV CC           : Router-Alert
    VCCV BFD          : Fault Detection with BFD
    Flow Label        : -
    Tunnel Group ID   : 0x800000130000001
    Tunnel NHLFE IDs  : 3
VSI Name: aaa
  Link ID: 8
    PW Type         : VLAN                  PW State : Up
    In Label        : 1272                  Out Label: 1275
    MTU             : 1500
    PW Attributes   : Main
    VCCV CC         : -
    VCCV BFD        : Fault Detection with BFD
    Flow Label      : -
    Tunnel Group ID : 0x960000000
    Tunnel NHLFE IDs: 1034
```

○ 若入、出标签取值为空或者为“-”。请先执行 **display l2vpn pw verbose** 命令查看 PW 使用的信令协议（Signaling Protocol），再修改建立 PW 的信令协议相关配置是否正确：

- 若信令协议为 BGP，则需要检查并修改 BGP 相关配置；
- 若信令协议为 LDP，则需要检查并修改 LDP 相关配置；
- 若信令协议为 Static，则需要检查并修改静态 PW 配置。

有关 PW 信令协议相关配置的详细介绍，请参见产品手册的“MPLS 配置指导”中的“MPLS L2VPN”和“VPLS”。

○ 若 Tunnel NHLFE IDs 取值为空，请继续执行第(3)步。

- 若 PW 的转发信息正常，请继续执行第(4)步。

(3) 执行 **display mpls lsp** 命令，查看是否存在承载 PW 的隧道，即是否存在 FEC 为 PW 对端 IP 地址的 LSP，若不存在，则需要先完成承载 PW 的隧道的建立。

```
<Sysname> display mpls lsp
FEC                         Proto    In/Out Label    Out Inter/NHLFE/LSINDEX
100.100.100.100/24          LDP      -/1049          GE1/0/1
```

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

- L2VPN/2/L2VPN_PWSTATE_CHANGE
- L2VPN/4/L2VPN_BGPVC_CONFLICT_LOCAL
- L2VPN/4/L2VPN_BGPVC_CONFLICT_REMOTE
- L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH
- L2VPN/2/L2VPN_HARD_RESOURCE_RESTORE
- L2VPN/4/L2VPN_LABEL_DUPLICATE

11.3 MPLS L3VPN故障处理

11.3.1 L3VPN 流量中断

1. 故障描述

经过 MPLS L3VPN 网络转发的私网流量中断。

2. 常见原因

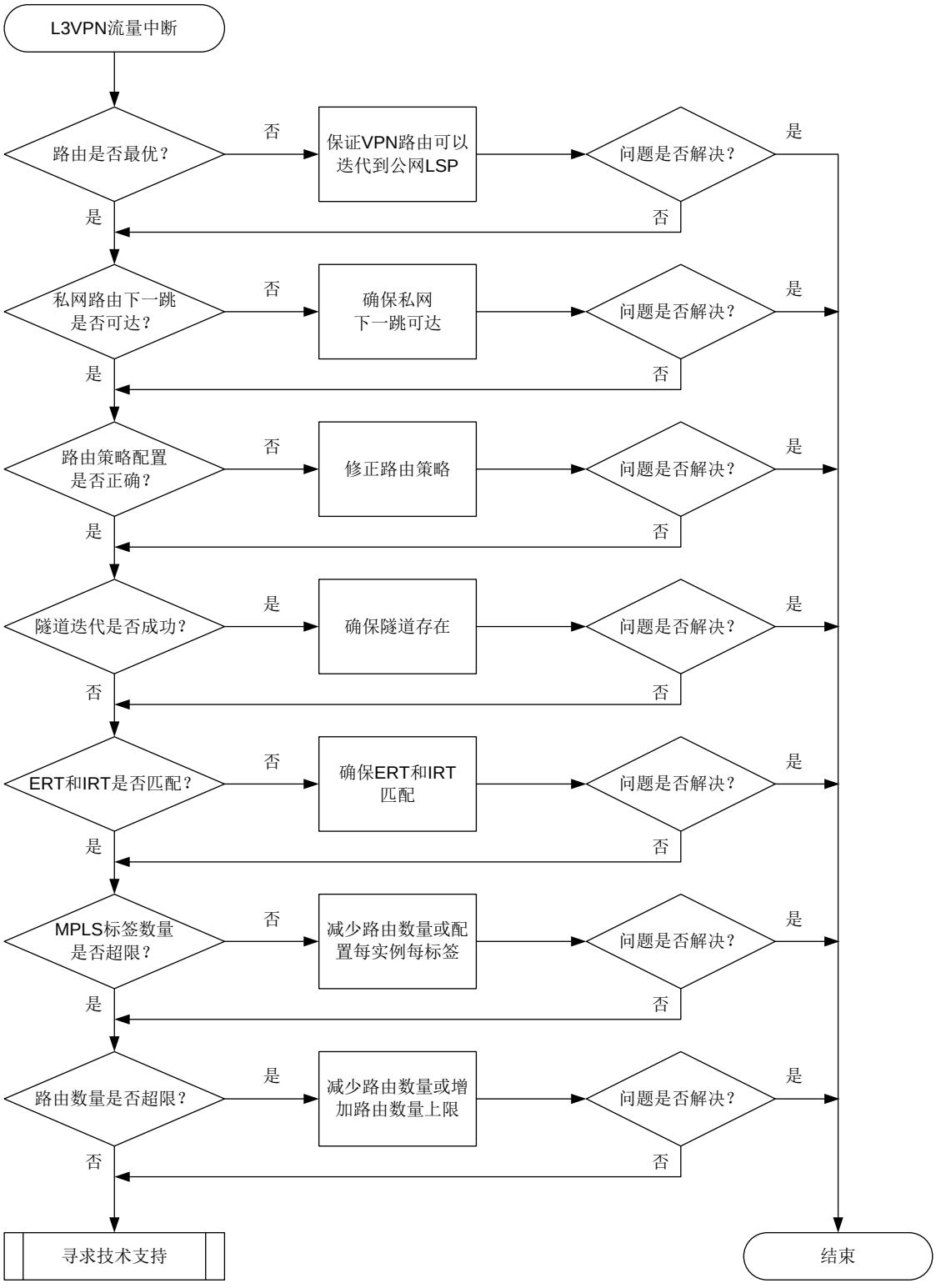
本类故障的常见原因主要包括：

- 私网路由下一跳不可达。
- 路由策略配置不当导致路由无法发布和接收。
- 标签超限导致私网路由无法发布。
- 私网路由迭代不到隧道。
- Export RT 和 Import RT 不匹配导致路由无法学习到私网路由表中。
- 路由超限导致收到的路由被丢弃。

3. 故障分析

本类故障的诊断流程如图 66 所示。

图66 L3VPN 流量中断故障诊断流程图



4. 处理步骤

(1) 检查路由是否为最优路由。

执行命令**display bgp routing-table vpnv4**或**display bgp routing-table vpnv6**命令，查看BGP VPNv4/VPNv6路由表中到达VPNv4/VPNv6邻居的BGP路由是否最优。

以路由100.1.2.0/24为例，路由信息中存在标记“>”，则表示该路由为最优路由。

```
<Sysname> display bgp routing-table vpnv4

 BGP local router ID is 1.1.1.9
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a – additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Total number of VPN routes: 8
 Total number of routes from all PEs: 8

 Route distinguisher: 100:1(vpn1)
 Total number of routes: 6

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* > 1.1.1.0/24          1.1.1.1         0                     32768   ?
*   1.1.1.2/32          1.1.1.1         0                     32768   ?
* > 100.1.2.0/24        100.1.1.1       0          100        0       400i
```

根据以上显示信息进行判断：

- 如果不是最优路由，则执行**display mpls lsp**命令，查看是否存在指定路由的MPLS转发表项。如果不存在，则请在连接远端PE的公网接口下执行**mpls enable**和**mpls ldp enable**命令，开启MPLS功能和LDP功能，保证VPNv4路由可以迭代到公网LSP；如果存在，则执行步骤(2)。
- 如果是最优路由，则执行步骤(2)。

(2) 检查私网路由下一跳是否可达。

在路由的发送端（本端PE）执行**display bgp routing-table vpnv4** *ipv4-address* [*mask* | *mask-length*]命令查看私网路由信息（*ipv4-address*表示私网路由前缀），确认路由是否存在。

- 如果路由不存在，请确认CE路由是否发布到PE。在远端PE上执行**display bgp routing-table vpnv4 peer advertised-routes**或**display bgp routing-table vpnv6 peer advertised-routes**命令，查看远端PE是否将私网路由信息发布给本端PE，例如：

  ```
  <Sysname> display bgp routing-table vpnv4 peer 22.22.22.22 advertised-routes

   Total number of routes: 6

   BGP local router ID is 11.11.11.11
   Status codes: * - valid, > - best, d - dampened, h - history,
                 s - suppressed, S - stale, i - internal, e - external
                 a - additional-path
         Origin: i - IGP, e - EGP, ? - incomplete
  ```

```
Route distinguisher: 1:1
Total number of routes: 3

     Network            NextHop         MED        LocPrf             Path/Ogn

* >e 1.1.1.1/32         10.1.1.2        0          100                20i
* >e 7.7.7.7/32         10.1.1.2        0          100                20?
* >e 10.1.1.0/24        10.1.1.2        0          100                20?
```

如果不存在以上显示信息，则执行步骤(3)。

- 如果路由存在，请确认私网路由下一跳是否可达，且私网路由是否活跃。

  查看 State 字段，如果取值包括 valid，则表示该路由是活跃的。查看 Original nexthop 字段，如果存在下一跳信息，则表示私网路由下一跳可达。

  - 如果私网路由不活跃，则执行 **display ip routing-table vpn-instance** *vpn-instance-name ip-address* 命令查看 IP 路由表中是否存在到 BGP 下一跳（Original nexthop）的路由。如果不存在，则说明私网路由下一跳不可达，请检查 PE 之间的公网路由配置；如果存在，则说明 BGP 路由下一跳可达，请执行步骤(3)。
  - 如果私网路由活跃，则执行步骤(3)。

```
<sysname> display bgp routing-table vpnv4 6.0.0.9 32

 BGP local router ID: 4.0.0.9
 Local AS number: 200


 Route distinguisher: 103:1
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of 6.0.0.9/32:
 From            : 3.0.0.9  (3.0.0.9)
 Rely nexthop    : 20.0.2.1
 Original nexthop: 3.0.0.9
 OutLabel        : 24128
 Ext-Community   : <RT: 100:1>
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 300 103
 Origin          : igp
 Attribute value : pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 Tunnel policy   : tp1
 Rely tunnel IDs : 2
```

(3) 检查路由策略是否正确。

在路由的发送端和接收端执行 **display current-configuration configuration bgp** 命令查看 BGP 配置，确认是否配置邻居的出方向和入方向策略。

```
<sysname> display current-configuration configuration bgp
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack1
 #
 address-family vpnv4
  peer 3.3.3.3 enable
  peer 3.3.3.3 route-policy in import
  peer 3.3.3.3 route-policy out export
#
return
```

如果两端配置了出方向和入方向策略，则需要确认这些策略是否会把私网路由过滤掉，导致该路由无法正常收发。

如果两端没有配置相应的出方向和入方向策略，或者路由策略没有过滤掉私网路由，则执行步骤(4)。

(4) 检查路由是否能迭代到隧道。

在路由的接收端（远端 PE）执行 **display bgp routing-table vpnv4** *ipv4-address* [*mask* | *mask-length*]命令查看 VPNv4 路由，确认 VPNv4 路由是否可以迭代到隧道。

如果显示信息中存在 Rely tunnel IDs 字段，则表示该路由可以迭代到隧道。

- 如果迭代不到隧道，则请参见“LDP LSP 无法 Up”故障进行定位。
- 如果迭代到隧道，则执行步骤(5)。

```
<sysname> display bgp routing-table vpnv4 6.0.0.9 32

 BGP local router ID: 4.0.0.9
 Local AS number: 200


 Route distinguisher: 103:1
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of 6.0.0.9/32:
 From            : 3.0.0.9  (3.0.0.9)
 Rely nexthop    : 20.0.2.1
 Original nexthop: 3.0.0.9
 OutLabel        : 24128
 Ext-Community   : <RT: 100:1>
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 300 103
 Origin          : igp
 Attribute value : pref-val 0
```

```
State           : valid, external, best
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
Tunnel policy   : tp1
Rely tunnel IDs : 2
```

(5) 检查是否 Export RT 和 Import RT 不匹配导致路由无法学习到私网路由表中。

在路由的发送端（本端 PE）和接收端（远端 PE）执行 **display bgp routing-table vpnv4** 和 **display current-configuration configuration vpn-instance** 命令，查看是否本端 VPN 实例的 Export RT 与远端 VPN 实例的 Import RT 不匹配，导致路由发送到远端 PE 后无法学习到远端 VPN 实例中。

在本端 PE 上执行 **display bgp routing-table vpnv4** 和 **display ip extcommunity-list** 命令查看本端 VPN 实例的 ERT 是否被过滤，导致路由无法发布。

- 如果 Export RT 和 Import RT 不匹配，则请在 VPN 实例下执行 **vpn-target** 命令配置匹配的 RT 值。
- 如果 Export RT 被路由策略过滤，则请在路由策略视图下执行 **apply extcommunity rt** 命令修改路由策略，取消过滤指定的 RT 属性。
- 如果 Export RT 和 Import RT 匹配，或者 Export RT 未被路由策略过滤，则执行步骤(6)。

查看路由携带的 ERT：

```
<sysname> display bgp routing-table vpnv4 6.0.0.9 32

 BGP local router ID: 4.0.0.9
 Local AS number: 200


 Route distinguisher: 103:1
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP routing table information of 6.0.0.9/32:
 From            : 3.0.0.9  (3.0.0.9)
 Rely nexthop    : 20.0.2.1
 Original nexthop: 3.0.0.9
 OutLabel        : 24128
 Ext-Community   : <RT: 100:1>
 RxPathID        : 0x0
 TxPathID        : 0x0
 AS-path         : 300 103
 Origin          : igp
 Attribute value : pref-val 0
 State           : valid, external, best
 IP precedence   : N/A
 QoS local ID    : N/A
 Traffic index   : N/A
 Tunnel policy   : tp1
 Rely tunnel IDs : 2
```

查看 BGP 扩展团体属性列表信息：

```
<sysname> display ip extcommunity-list 1
Extended Community List Number 10
        Deny   rt: 100:1
Extended Community List Number 20
        Permit rt: 200:1
```

查看本地配置的 IRT：

```
<sysname> display current-configuration configuration vpn-instance
#
ip vpn-instance vpn1
 route-distinguisher 1:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
```

(6) 检查 MPLS 标签数量是否超限。

在路由发送端（本端 PE）执行 **display mpls interface** 命令确认与远端 PE 相连的公网接口是否开启了 MPLS 功能。

- 如果显示信息中存在与远端 PE 相连的公网接口，则表示与远端 PE 相连的公网接口开启了 MPLS 功能。
- 如果显示信息中不存在与远端 PE 相连的公网接口，则在与远端 PE 相连的公网接口视图下执行 **mpls enable** 命令，开启 MPLS 功能。

```
<Sysname> display mpls interface
Interface               Status       MPLS MTU
GE1/0/1                 Up           1500
GE1/0/2                 Up           1500
```

使用 **display bgp routing-table vpnv4 advertise-info** 命令查看路由发送时是否申请标签。

- 如果显示信息中 Inlabel 字段无取值，则可能是由于标签资源不足，导致无法为该路由申请标签。如果是标签不足，则可以通过以下方法减少标签的使用量：
  - 在 VPN 实例视图下执行 **apply-label per-instance** 命令配置每实例每标签。
  - 通过路由聚合来减少路由数量。
  - 在系统视图下执行 **mpls max-label** 命令增加设备可分配的标签数量。
- 如果显示信息中 Inlabel 字段有合理值，则表示标签资源充足，已经为该路由申请标签，请执行步骤(7)。

```
<Sysname> display bgp routing-table vpnv4 10.1.1.0 24 advertise-info

BGP local router ID: 1.1.1.9
Local AS number: 100


Route distinguisher: 100:1
Total number of routes: 1
Paths:   1 best

BGP routing table information of 10.1.1.0/24(TxPathID:0):
```

```
Advertised to VPN peers (1 in total):
 3.3.3.9
Inlabel       : 1279
```

(7) 检查路由数量是否超限。

执行 **display bgp peer vpnv4 log-info** 命令，查看指定对等体的日志信息。如果显示 Cease/maximum number of VPNv4 prefixes reached，则表示路由数量超规格。

```
<Sysname> display bgp peer vpnv4 1.1.1.1 log-info

 Peer : 1.1.1.1

     Date      Time    State Notification
                             Error/SubError

  06-Feb-2013 22:54:42 Down  Send notification with error 6/1
                             Cease/maximum number of VPNv4 prefixes reached
```

如果设备上打印如下日志信息，则表示路由数量超规格。

```
BGP/4/BGP_EXCEED_ROUTE_LIMIT: BGP default.vpn1: The number of routes (101) from peer
1.1.1.1 (IPv4-UNC) exceeds the limit 100.
BGP/4/BGP_REACHED_THRESHOLD: BGP default.vpn1: The ratio of the number of routes (3)
received from peer 1.1.1.1 (IPv4-UNC) to the number of allowed routes (2) has reached
the threshold (75%).
```

- 如果路由数量超规格，则在路由接收端的 VPNv4 地址族视图或者 VPNv6 地址族视图下执行 **peer route-limit** 命令调大允许从对等体接收路由的最大数目。
- 如果路由数量未超规格，则执行步骤(8)。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：BGP4-MIB

- bgpBackwardTransition (1.3.6.1.2.1.15.7.2)

相关日志

- BGP_EXCEED_ROUTE_LIMIT
- BGP_REACHED_THRESHOLD

11.3.2 L3VPN 私网路由频繁震荡

1. 故障描述

远端 PE 发布的私网路由在本端 PE 上频繁震荡。

2. 常见原因

本类故障的常见原因主要包括：

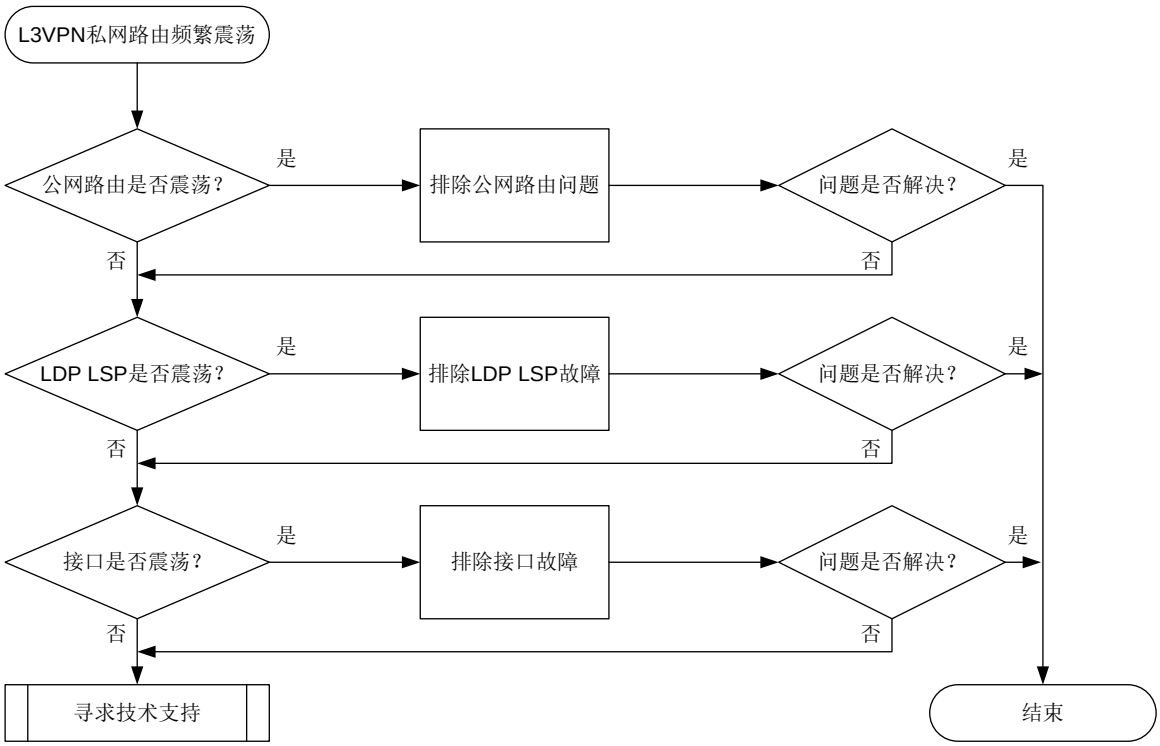
- 公网路由震荡

- LDP LSP 震荡
- 接口震荡

3. 故障分析

本类故障的诊断流程如图 67 所示。

图67 L3VPN 私网路由频繁震荡故障诊断流程图



4. 处理步骤

(1) 检查公网路由是否震荡。

a. 确认路由类型。

执行 **display ip routing-table** 命令查看路由类型。

以如下显示为例，Proto 字段显示为 IS_L1，表示路由类型为 IS-IS；Interface 字段显示为 Tun1，表示部署了 LDP over MPLS TE。

```
<Sysname> display ip routing-table 1.1.1.1

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
1.1.1.1/32          IS_L1   15  10          1.1.1.1         Tun1
```

b. 查看路由是否震荡。

根据路由类型，判断路由是否震荡。以 IS-IS 为例，执行 **display ip routing-table protocol isis** 命令，查看路由信息。如果路由信息一直在显示和不显示两种情况切换，则表示路由震荡。

- 如果路由震荡，请按照路由类型，参见“OSPF 邻居 Down”、“OSPFv3 邻居 Down”或“IS-IS 路由震荡”故障处理，排除路由问题。
- 如果路由没有震荡，请执行步骤(2)。

(2) 检查 LDP LSP 是否震荡。

建议每 1 秒执行一次 **display mpls ldp peer** 命令，连续执行 5～10 次，查看显示信息的 State 字段。如果该字段的取值在 Operational 状态和其他状态之间切换，则表示 LDP 会话震荡，导致 LDP LSP 震荡。

- 如果 LDP LSP 震荡，则请参见“LDP LSP 震荡”故障进行定位。
- 如果 LDP LSP 没有震荡，则执行步骤(3)。

```
<Sysname> display mpls ldp peer
VPN instance: public instance
Total number of peers: 1
Peer LDP ID            State         Role     GR   AUT       KA Sent/Rcvd
1.1.1.1:0              Operational   Active   Off  None      298/298
```

(3) 检查接口是否震荡。

执行 **display interface brief** 命令，查看 Link 和 Protocol 字段。Link 和 Protocol 字段均显示 Up，则表示接口状态为 Up，否则表示接口状态为 Down。若接口一直在 Up 和 Down 两种状态间切换，则表示接口震荡。

- 如果接口震荡，则请参见“接口不 UP”故障进行定位。
- 如果接口没有震荡，请执行步骤(4)。

```
<Sysname> display interface gigabitethernet 1/0/1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) – spoofing

Interface                         Link Protocol Primary IP      Description
GE1/0/1                           UP   UP       --
```

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11.3.3 PE 间无法交换 VPN 路由

1. 故障描述

PE 间无法交换 VPNv4 或 VPNv6 路由。

2. 常见原因

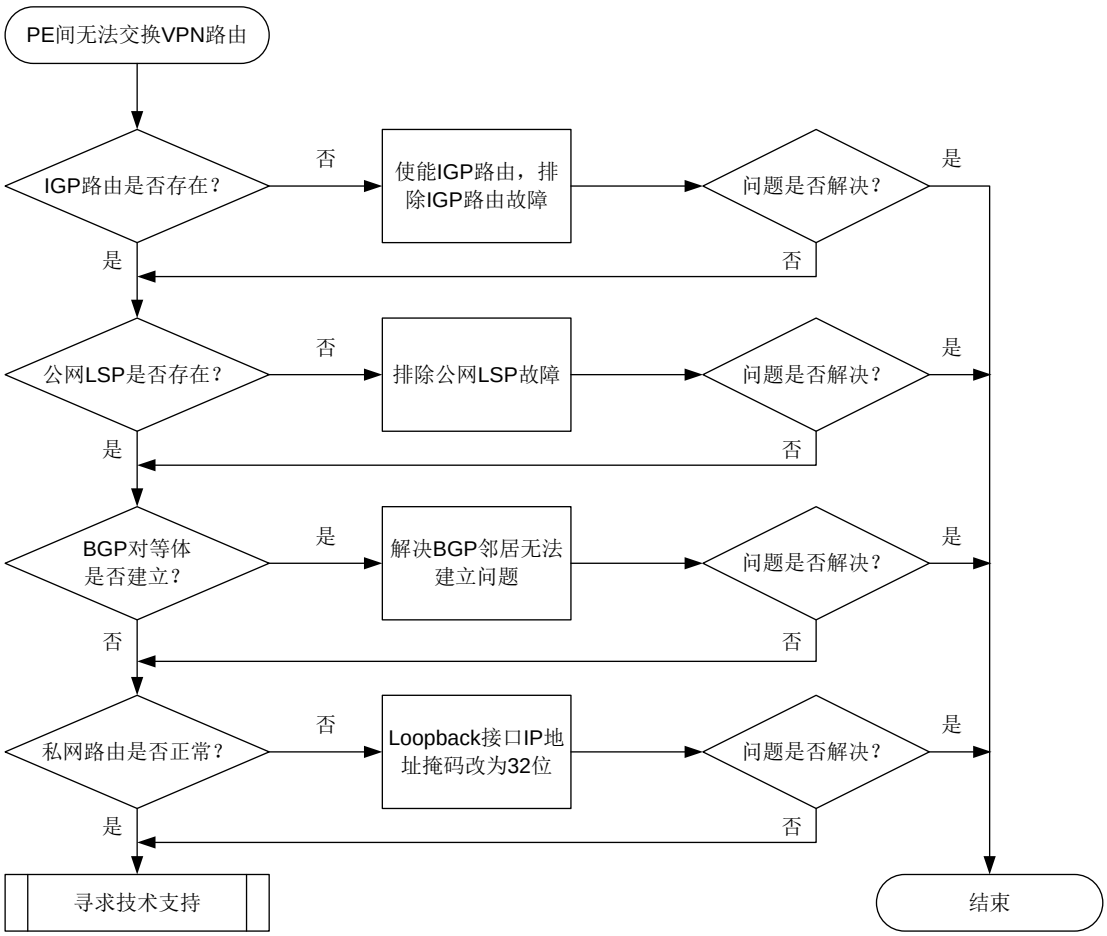
本类故障的常见原因主要包括：

- 公网 IGP 路由未发布
- 公网 LSP 不存在
- BGP 对等体未建立
- 未学习到 VPNv4 或 VPNv6 路由

3. 故障分析

本类故障的诊断流程如图 68 所示。

图68 PE 间无法交换私网路由故障诊断流程图



4. 处理步骤

(1) 检查 IGP 路由是否存在。

执行 **display ip routing-table** 命令，查看是否存在到达对端 PE 的 Loopback 接口的网段路由：

```
<Sysname> display ip routing-table 1.1.1.1

Summary count : 1
```

```
Destination/Mask    Proto   Pre Cost        NextHop         Interface
1.1.1.2/32          IS_L1   15  10          1.1.1.1         LoopBack1
```

- 如果不存在，则在 Loopback 接口和公网接口下使能 IGP 协议，确保发布对应网段路由。
- 如果存在，则执行步骤(2)。

(2) 检查公网 LSP 是否存在。

执行 **display mpls lsp** 命令，查看是否存在到达远端 PE 的 Loopback 接口的公网 LSP：

- 如果不存在，则在公网接口下使能 MPLS 功能和 MPLS LDP 功能，确保建立公网 LSP。
- 如果存在，则执行步骤(3)。

```
<Sysname> display mpls lsp
FEC                         Proto    In/Out Label    Out Inter/NHLFE/LSINDEX
1.1.1.2/32                  LDP      -/1049          GE1/0/1
<Sysname> display mpls lsp
FEC                         Proto    In/Out Label    Out Inter/NHLFE/LSINDEX
1.1.1.1/24                  LDP      -/1051          GE1/0/1
```

执行 **display mpls ldp peer verbose** 命令，查看 LDP 会话是否成功建立：

- 如果 State 字段显示不是 Operational，则表示 LDP 会话没有正常建立，请参见“LDP 会话无法 Up”故障进行定位。
- 如果 State 字段的显示为 Operational，则表示 LDP 会话已建立并处于 Up 状态，请执行步骤(3)。

```
<Sysname> display mpls ldp peer verbose
VPN instance: public instance
 Peer LDP ID      : 1.1.1.1:0
 Local LDP ID     : 2.2.2.2:0
 TCP Connection   : 2.2.2.2:14080 -> 1.1.1.1:646
 Session State    : Operational       Session Role     : Active
 Session Up Time  : 0000:00:14 (DD:HH:MM)
…
```

(3) 检查 BGP 对等体关系是否建立。

执行 **display bgp peer vpnv4** 命令，查看 PE 之间 BGP VPNv4 对等体关系，并执行 **display bgp peer ipv4 vpn-instance** 命令，查看 PE 与 CE 之间 BGP 对等体关系：

- 如果不存在 BGP 对等体关系，或者 State 字段显示不是 Established，则表示未建立 BGP 对等体关系，请参见“BGP 邻居无法建立”故障进行定位。
- 如果 State 字段的显示为 Established，则表示已建立 BGP 对等体关系，请执行步骤(4)。

```
<Sysname> display bgp peer vpnv4

 BGP local router ID: 192.168.100.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State

 1.1.1.2                200       13       16    0        0 00:10:34 Established
<Sysname> display bgp peer ipv4 vpn-instance vpn1
```

```
BGP local router ID: 1.1.1.1
Local AS number: 100
Total number of peers: 1                 Peers in established state: 1

* - Dynamically created peer
Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State

10.1.1.1            65410        5        4    0        1 00:01:19 Established
```

(4) 检查私网路由是否正常。

执行 **display ip routing-table vpn-instance** 命令，查看私网路由：

- 如果私网路由的掩码不是 32 位，且发现该路由的协议不是 BGP 协议，则表示两端 PE 的 Loopback 接口的 IP 地址在同一网段，设备将优选直连路由，而不是私网路由。请修改 PE 上的 Loopback 接口的 IP 地址，将掩码修改为为 32 位。
- 如果私网路由的掩码是 32 位，且发现该路由的协议是 BGP 协议，则私网路由正常，请执行步骤(5)。

```
<Sysname> display ip routing-table vpn-instance vpn1

Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
1.1.1.0/24          Direct  0   0           1.1.1.1         LoopBack1
```

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

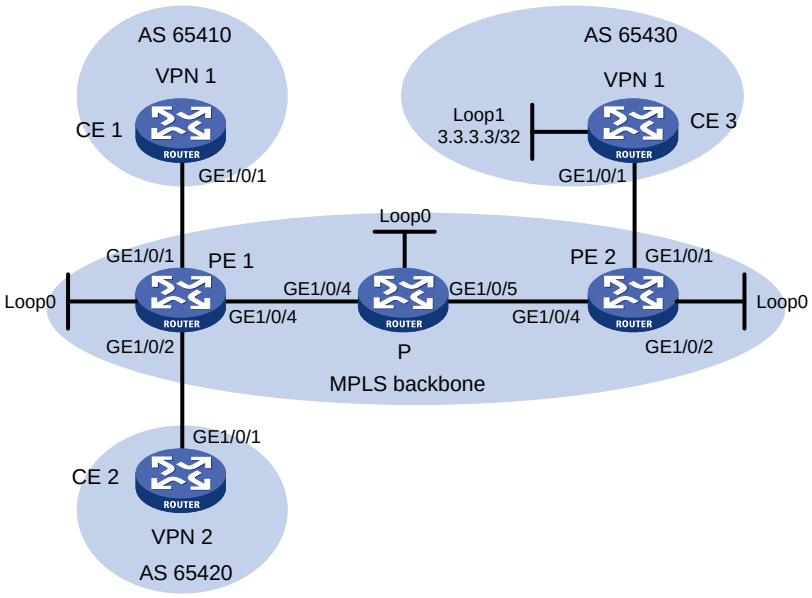
11.3.4 配置相同 RT 的不同 VPN 之间不能互通

1. 故障描述

在图69的网络中，配置MPLS L3VPN业务，CE 1与CE 3属于VPN 1，CE 2属于VPN 2。由于业务的需求，在VPN 1和VPN 2上配置了相同的Route Target，以实现不同VPN间互通。

配置完成后，发现CE 1可以Ping通相同VPN的CE 3（IP地址为3.3.3.3），但CE 2无法Ping通不同VPN的3.3.3.3。

图69 MPLS L3VPN 组网图



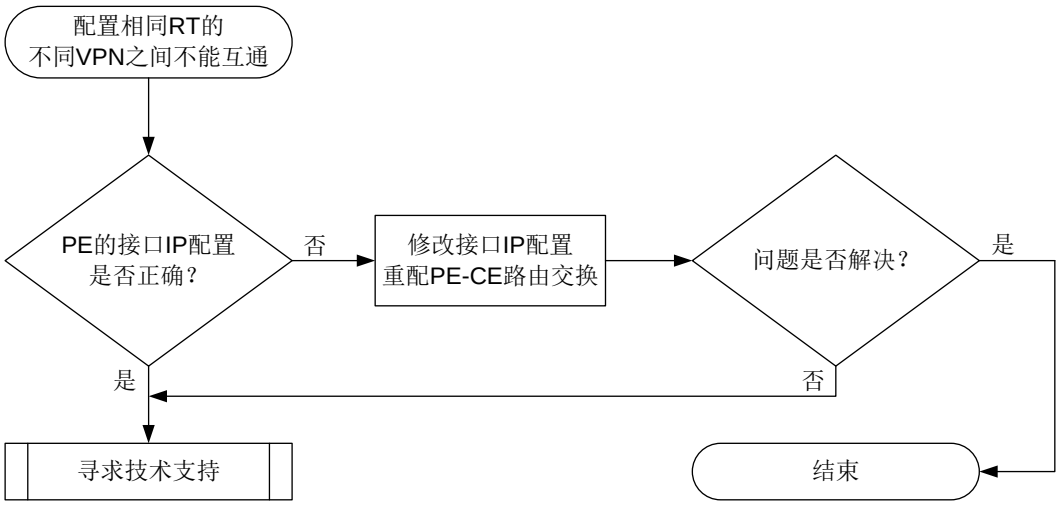
2. 常见原因

本场景中，CE 1 可以 Ping 通相同 VPN 的 CE 3，说明 MPLS 骨干网中进行标签转发的公网隧道正常，本类故障的常见原因仅包括：PE 设备上不同的 VPN 实例绑定的 IP 地址存在冲突。

3. 故障分析

本类故障的诊断流程如图 70 所示。

图70 配置相同 RT 的不同 VPN 之间不能互通的故障诊断流程图



4. 处理步骤

(1) 检查 PE 的接口 IP 是否存在冲突。

在 PE 1 上执行 **display ip interface brief** 命令查看接口的 IP 地址，例如：

```
<Sysname> display ip interface brief
```

```
*down: administratively down
(s): spoofing  (l): loopback
Interface          Physical Protocol IP Address/Mask    VPN instance Description
...
GE1/0/1            up       up       10.1.1.1/24        vpn1         --
GE1/0/2            up       up       10.1.1.1/24        vpn2         --
...
```

如果不同 VPN 实例的接口 IP 地址不相同，请执行步骤（2）。

如果不同 VPN 实例的接口 IP 相同，则修改其中一个 VPN 实例中 PE 上的接口以及与其相连的 CE 上的接口的 IP 地址，并重新配置 PE 设备与 CE 设备间的路由交换。

由于 BGP 会将 RT 匹配的路由在 VPN 实例间进行互引，为不同 VPN 的接口设置相同 IP 地址时，同一目的地址的路由在 BGP 路由表中将会出现两条，而 BGP 只会优选其中一条，例如：

```
<Sysname> display bgp routing-table vpnv4

 BGP local router ID is 11.11.11.11
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

 Total number of VPN routes: 11
 Total number of routes from all PEs: 2

 Route distinguisher: 1:1(vpn1)
 Total number of routes: 6

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 1.1.1.1/32         10.1.1.2        0                     0       20i
* >e 2.2.2.2/32         10.1.1.2        0                     0       30i
* >i 3.3.3.3/32         22.22.22.22     0          100        0       40i
* >e 10.1.1.0/24        10.1.1.2        0                     0       20?
* >i 30.1.1.0/24        22.22.22.22     0          100        0       40?

 Route distinguisher: 2:2(vpn2)
 Total number of routes: 5

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 1.1.1.1/32         10.1.1.2        0                     0       20i
* >e 2.2.2.2/32         10.1.1.2        0                     0       30i
* >i 3.3.3.3/32         22.22.22.22     0          100        0       40i
* >e 10.1.1.0/24        10.1.1.2        0                     0       20?
*  e                    10.1.1.2        0                     0       30?
* >i 30.1.1.0/24        22.22.22.22     0          100        0       40?
```

如上所示，在 RD 为 2:2 的 VPN 实例（即 VPN 2）BGP 路由表中，优选的 10.1.1.0 网段的路由来自 VPN 1（根据 AS_PATH 属性判断），VPN 2 发布的路由未被优选，所以从 VPN 1 去

往 VPN 2 的流量不会被 PE 1 从 GigabitEthernet1/0/2 接口发送给 VPN 2，而是从 GigabitEthernet1/0/1 接口发送给 VPN 1，导致跨 VPN 通信失败。

所以，将关联了 VPN 实例的接口以及与其相连的 CE 上的接口修改为不同的 IP 地址，可以解决这类问题。以 PE-CE 间通过 EBGP 会话交互路由为例，PE 1 的处理步骤如下：

a. 在系统视图下，执行 **interface** 命令进入关联了 VPN 实例的接口视图。
b. 执行 **ip address** 命令修改接口的 IP 地址。
c. 在系统视图下，执行 **bgp** 命令进入 BGP 实例视图。
d. 执行 **ip vpn-instance** 命令进入 BGP-VPN 实例视图。
e. 执行 **undo peer** 命令删除用原冲突 IP 地址建立的 BGP 对等体。
f. 执行 **peer as-number** 命令，指定使用新 IP 地址的 CE 设备为 EBGP 对等体。
g. 执行 **address-family ipv4 unicast** 命令，进入 BGP IPv4 单播地址族视图。
h. 执行 **peer enable** 命令，使能与 CE 设备交互 BGP IPv4 单播路由信息的能力。

假设仅修改了 VPN 2 的 IP 地址，则 CE 2 的处理步骤如下：

a. 在系统视图下，执行 **interface** 命令进入与 PE 1 直连的接口视图。
b. 执行 **ip address** 命令修改接口的 IP 地址。
c. 在系统视图下，执行 **bgp** 命令进入 BGP 实例视图。
d. 执行 **undo peer** 命令删除用原冲突 IP 地址建立的 BGP 对等体。
e. 执行 **peer as-number** 命令，指定使用新 IP 地址的 PE 设备为 EBGP 对等体。
f. 执行 **address-family ipv4 unicast** 命令，进入 BGP IPv4 单播地址族视图。
g. 执行 **peer enable** 命令，使能与 PE 设备交互 BGP IPv4 单播路由信息的能力。
h. 执行 **import-route** 命令或 **network** 命令，发布 VPN 实例的路由信息。

如果故障仍然未能排除，请执行步骤（2）。

(2) 请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11.3.5 路由反射器进行 VPN-Target 过滤导致 PE 无法学习到路由

1. 故障描述

PE 设备发布的 MVPN 路由、VPNv4/VPNv6 路由、BGP L2VPN 信息、VPN Flowspec 路由以及 EVPN 路由无法通过路由反射器反射给远端 PE。

2. 常见原因

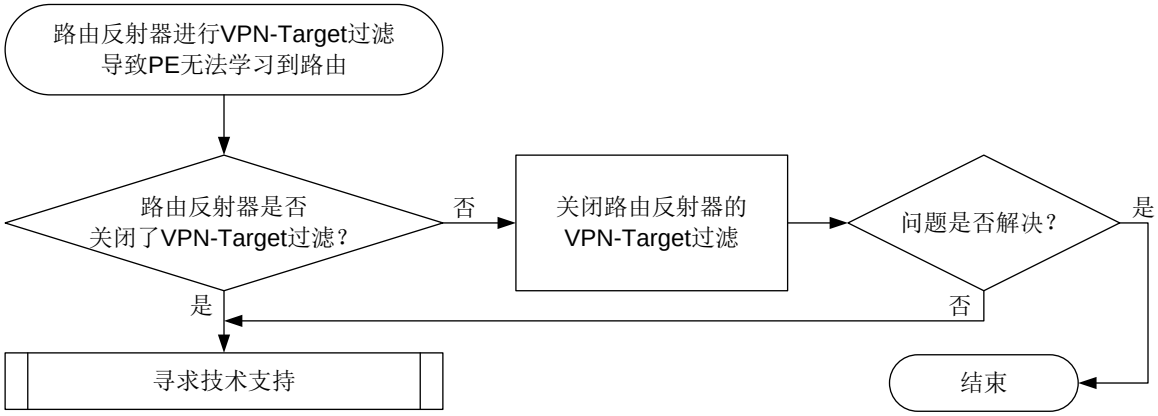
路由反射器缺省会对 MVPN 路由、VPNv4/VPNv6 路由、BGP L2VPN 信息、VPN Flowspec 路由以及 EVPN 路由进行 VPN-Target 过滤，即只将 Export Route Target 属性与本地 Import Route Target

属性匹配的路由信息加入到路由表。路由反射器上不存在与接收路由匹配的 Route Target 时，接收到的路由将被丢弃，导致无法转发该路由信息给远端 PE。

3. 故障分析

关闭路由反射器的 VPN-Target 过滤功能，可以解决本类故障，本故障的处理流程如图 71 所示。

图71 路由反射器进行 VPN-Target 过滤导致 PE 无法学习到路由故障处理流程



4. 处理步骤

(1) 检查对应地址族配置，确保配置了 undo policy vpn-target 命令：

a. 在 BGP 实例视图下，执行 display this 命令，查看在各地址族视图下是否存在 undo policy vpn-target 配置。如果不存在，请执行步骤 b；如果存在，请执行步骤（2）。

b. 进入相应的地址族视图，通过 undo policy vpn-target 命令关闭 VPN-Target 过滤，使得路由反射器可以转发 RT 不匹配的路由信息。如果故障仍不能排除，请执行步骤（2）。

(2) 请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11.3.6 PE 的私网 IP 路由表中没有远端 PE 发布的路由

1. 故障描述

在 MPLS L3VPN/IPv6 MPLS L3VPN 网络中，PE 的 VPN 实例 IP 路由表中没有远端 PE 用户站点的私网路由，导致 CE 间无法互通。

2. 常见原因

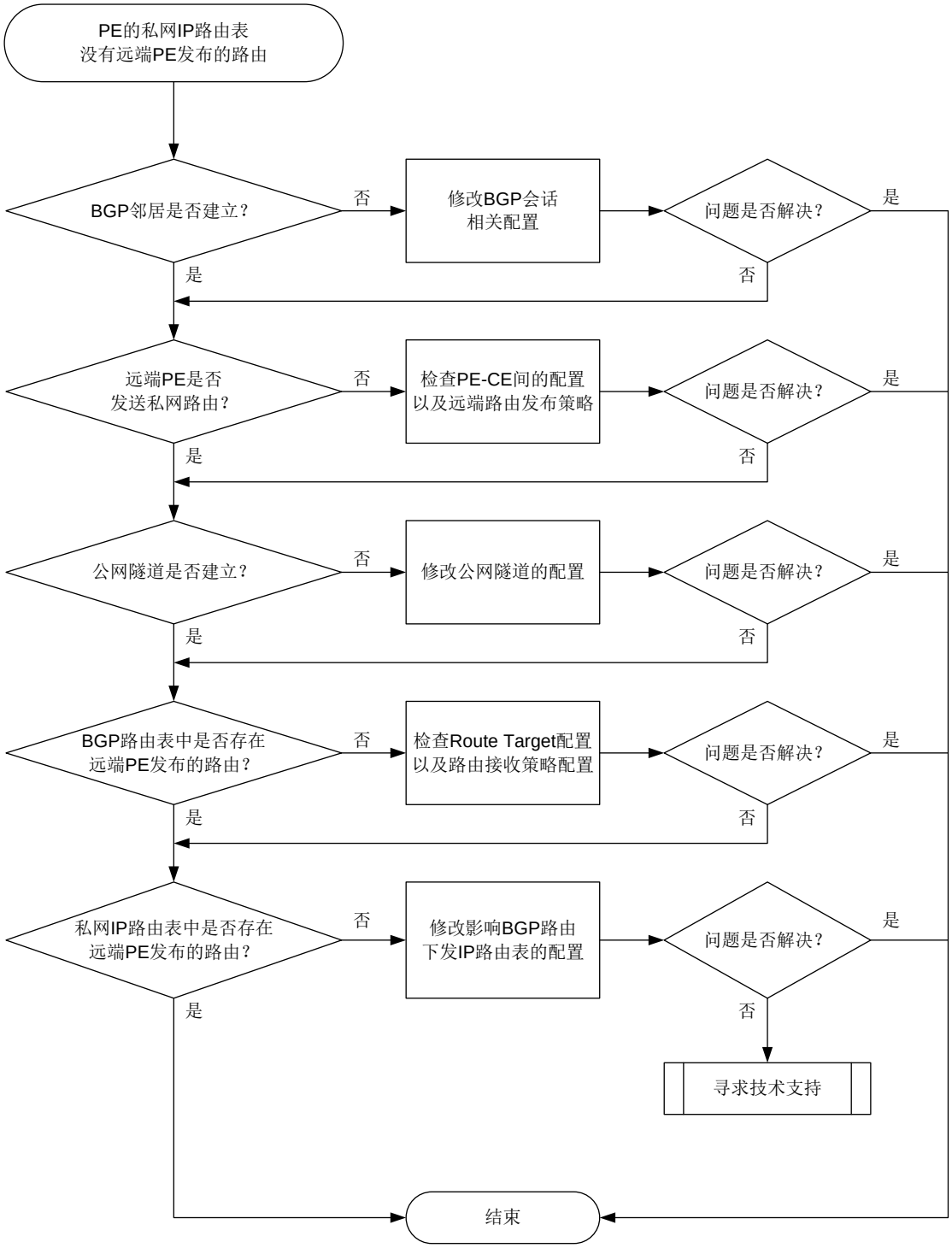
本类故障的常见原因主要包括：

- 与远端 PE 的 BGP 会话未进入 Established 状态。
- 远端 PE 未发送私网路由。
- 公网隧道未建立。
- 远端 PE 发送的私网路由被本端丢弃。
- 远端 PE 发送的私网路由在本端的 BGP 路由表中，但未被添加到 VPN 实例的 IP 路由表中。

3. 故障分析

本类故障的诊断流程如图 72 所示。

图72 PE 的私网 IP 路由表中没有远端 PE 发布的路由故障诊断流程图



4. 处理步骤

(1) 检查 BGP 邻居是否建立。

执行 **display bgp peer vpnv4** 或 **display bgp peer vpnv6** 命令，查看本端 PE 与远端 PE 是否建立起了处于 Established 状态的 BGP 会话，例如：

```
<Sysname> display bgp peer vpnv4

 BGP local router ID: 11.11.11.11
 Local AS number: 10
 Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State

 22.22.22.22             10       82       69    0        2 01:01:28 Established
```

- 如果已经建立，请执行步骤（3）。
- 如果未建立，请参见“三层技术-IP 路由类故障处理”手册中的“BGP 会话无法进入 Established 状态”进行定位。BGP 会话进入 Established 状态后，如果故障仍未能排除，请执行步骤（2）。

(2) 查看远端 PE 是否向本端发布了私网路由信息。

在远端 PE 上执行 **display bgp routing-table vpnv4 peer advertised-routes** 或 **display bgp routing-table vpnv6 peer advertised-routes** 命令，查看远端 PE 是否将私网路由信息发布给本端 PE，例如：

```
<Sysname> display bgp routing-table vpnv4 peer 22.22.22.22 advertised-routes

 Total number of routes: 6

 BGP local router ID is 11.11.11.11
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 1:1
 Total number of routes: 3

     Network            NextHop         MED        LocPrf             Path/Ogn

* >e 1.1.1.1/32         10.1.1.2        0          100                20i
* >e 7.7.7.7/32         10.1.1.2        0          100                20?
* >e 10.1.1.0/24        10.1.1.2        0          100                20?

 Route distinguisher: 2:2
 Total number of routes: 3

     Network            NextHop         MED        LocPrf             Path/Ogn

* >e 2.2.2.2/32         10.1.1.2        0          100                30i
* >e 7.7.7.7/32         10.1.1.2        0          100                30?
* >e 10.1.1.0/24        10.1.1.2        0          100                30?
```

如果存在这样的信息，请执行步骤（3），如果不存在，则进行如下检查：

a. 在远端 PE 上执行 display bgp routing-table vpnv4 或 display bgp routing-table vpnv6 命令，查看是否存在想要发布的私网路由。
   - 如果存在，请执行步骤 b。
   - 如果不存在，则检查 PE-CE 间的配置。PE 与 CE 间可以使用多种协议交互路由信息，包括静态路由、RIP、OSPF、OSPFv3、IS-IS、BGP 等。关于 BGP 路由协议故障处理方法，请参见“三层技术-IP 路由类故障处理手册”中的“BGP 故障处理”；常见的 IGP 路由协议故障处理方法，请参见“三层技术-IP 路由类故障处理”手册中的“OSPF 故障处理”、“OSPFv3 故障处理”或“IS-IS 故障处理”。远端 PE 的 BGP 路由表获得了私网路由后，如果故障仍不能排除，请执行步骤 b。

b. 在远端 PE 的 BGP VPNv4 地址族视图或者 BGP VPNv6 地址族视图下执行 display this 命令，查看是否存在发布策略过滤了私网路由信息导致无法发布，可能造成影响的配置命令有：
   - **peer prefix-list export**
   - **peer filter-policy export**
   - **peer as-path-acl export**
   - **filter-policy export**
   - **peer route-policy export**

   可以通过执行上述命令的 undo 形式命令来取消对私网路由信息发布的过滤，为了避免组网中的其他配置受到影响，请在技术支持人员的引导下修改私网路由信息发布的过滤策略。

   如果故障仍不能排除，请执行步骤（3）。

(3) 查看公网隧道是否建立。

MPLS L3VPN 的公网隧道可以是 LSP 隧道、MPLS TE 隧道和 GRE 隧道。当公网隧道为 LSP 隧道或 MPLS TE 隧道时，公网标记为 MPLS 标签，称为公网标签；当公网隧道为 GRE 隧道时，公网标记为 GRE 封装。

常见的公网隧道建立方式是使用 LDP 标签分发协议自动建立标签转发路径，本故障处理流程以该方式为例，介绍建立公网隧道的故障排查方法。其他方式的公网隧道请参见相应的故障处理手册或寻求技术支持人员的帮助进行排查。

在私网路由发布的骨干网路径上，为所有设备执行 **display mpls ldp peer** 命令，查看是否与 LDP 对等体成功建立了会话，例如：

```
<Sysname> display mpls ldp peer
VPN instance: public instance
Total number of peers: 2
Peer LDP ID             State         Role     GR   AUT       KA Sent/Rcvd
22.22.22.22:0           Operational   Passive  Off  None      1816/1816
11.11.11.11:0           Operational   Passive  Off  None      1816/1816
```

如果已经成功建立了会话，请执行步骤（4）。

如果未建立 LDP 会话，请参见“MPLS 类故障处理手册”中的“LDP 会话 Down 的定位思路”进行排查。

如果公网隧道建立后，故障仍不能排除，请执行步骤（4）。

(4) 检查本端 PE 的 BGP 路由表中是否存在对端 PE 发布的私网路由。

在本端 PE 上执行 **display bgp routing-table vpnv4** 或 **display bgp routing-table vpnv6** 命令，查看是否存在远端 PE 发布的私网路由。

如果不存在，则执行如下操作：

a. 在本端 PE 和远端 PE 上，均执行 display ip vpn-instance instance-name 命令，查看本端 PE 的 VPN 实例的 Import VPN Targets 与远端 PE 的 Export VPN Targets 是否一致，显示信息举例如下。

```
<Sysname> display ip vpn-instance instance-name vpn1
  VPN-Instance Name and Index : vpn1, 1
  Route Distinguisher : 1:1
  Interfaces : GigabitEthernet1/0/1
  TTL mode: pipe
  Address-family IPv4:
   Export VPN Targets :
       1:1
   Import VPN Targets :
       1:1
```

   - 如果不一致，则需要在本端或者远端 PE 的 VPN 实例视图下通过 **vpn-target** 命令，将 RT 修改为匹配的值。修改 RT 后，如果本端 PE 的 BGP 路由表中仍未存在对端 PE 发布的私网路由，请执行步骤 b；如果本端 PE 的 BGP 路由表中已经存在对端 PE 发布的私网路由，但故障仍不能排除，请执行步骤（5）。
   - 如果一致，请执行步骤 b。

b. 通过在 BGP 实例视图下执行 display this 命令，查看是否存在接收策略过滤了私网路由信息导致无法接收，可能造成影响的配置命令有：

   - **peer prefix-list import**
   - **peer filter-policy import**
   - **peer as-path-acl import**
   - **filter-policy import**
   - **peer route-policy import**

   可以通过执行上述命令的 undo 形式命令来取消对私网路由信息接收的过滤，为了避免组网中的其他配置受到影响，请在技术支持人员的引导下修改私网路由信息接收的过滤策略。

如果故障仍不能排除，请执行步骤（5）。

(5) 检查 BGP 路由添加到 VPN 实例 IP 路由表的受阻原因。可能的原因有：

- 设备配置了 **undo policy vpn-target** 命令，与当前 VPN 实例 Route Target 属性不匹配的 VPNv4/VPNv6 路由可以添加到 VPN 实例的 BGP 路由表中，并能够在 BGP 路由表中被优选，但是这些路由无法添加到当前 VPN 实例的 IP 路由表中。在 BGP 实例视图下执行 **display this** 命令，查看配置了 **undo policy vpn-target** 命令的地址族，进入该地址族视图，并执行 **policy vpn-target** 命令，可以解决此问题。
- 设备配置了 **routing-table bgp-rib-only** 命令，,禁止 BGP 路由下发到 IP 路由表中。在 BGP 实例视图下执行 **display this** 命令，查看配置了 **routing-table bgp-rib-only** 命令的地址族，进入该地址族视图，并执行 **undo routing-table bgp-rib-only** 命令，可以解决此问题。

如果故障仍未能排除，请执行步骤（6）。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。

- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11.3.7 私网间大包不通

1. 故障描述

MPLS L3VPN/IPv6 MPLS L3VPN 网络中同时存在我司设备和其他厂商设备，用户访问跨站点的私网资源时，不能打开部分网站，也不能通过 FTP 下载文件。执行 **ping** 命令检验发现，在指定 ICMP 报文的净荷为 1464 字节以上时 Ping 不通，指定 ICMP 报文的净荷小于 1464 字节时，可以 Ping 通。

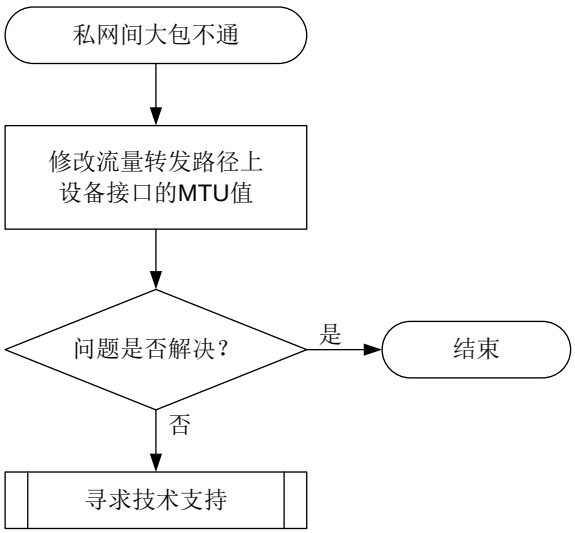
2. 常见原因

本类故障的常见原因主要为：流量转发路径上设备接口的 MTU 值过小。

3. 故障分析

本故障的处理流程如图 73 所示。

图73 私网间大包不通故障诊断流程图



4. 操作步骤

(1) 在流量转发路径上，将设备接口的 MTU 值修改为大于或等于 1508 字节。

- 在我司设备上，可通过 **display interface** 命令查看接口的 MTU。例如：

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: Administratively UP
Line protocol state: UP
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
```

```
Maximum transmission unit: 1500
...
```

需要修改接口的 MTU 值时，请在该接口视图下执行 **ip mtu** 或 **ipv6 mtu** 命令。

- 其他厂商的设备配置请参考相关的资料。

如果故障仍未能排除，请执行步骤（2）。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

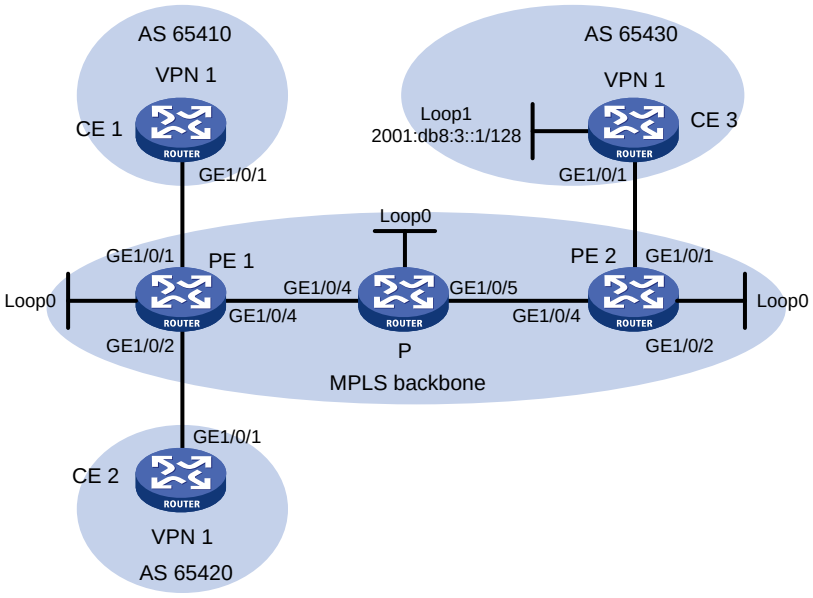
无

11.3.8 PE 设备 Ping 不通远端 CE 网段

1. 故障描述

如图 74 所示，在 IPv6 MPLS L3VPN 网络中，PE 1 上配置了多个接口关联同一个 VPN 实例 VPN 1。在 CE 1 和 CE 2 上执行 **ping ipv6 2001:db8:3::1** 命令，均能 Ping 通远端的 CE 3 网段，但在 PE 1 上执行 **ping ipv6 –vpn-instance vpn1 2001:db8:3::1** 命令时，Ping 不同 CE 3 网段。

图74 IPv6 MPLS L3VPN 组网图



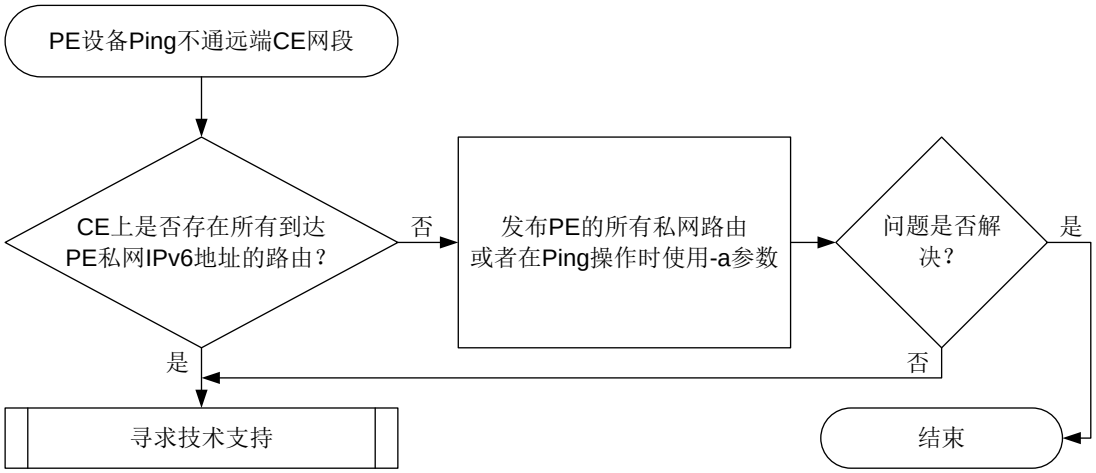
2. 常见原因

本类故障的常见原因主要为：CE 3 上没有到达 PE 1 所有私网 IPv6 地址的路由。私网 IPv6 地址的范围是，PE 1 上与 CE 3 相同的 VPN 实例中，所有处于 UP 状态的接口的 IPv6 地址。

3. 故障分析

本故障的处理流程如图 75 所示。

图75 PE 设备 Ping 不同远端 CE 网段故障诊断流程图



4. 操作步骤

(1) 检查 CE 3 上是否存在到达 PE 1 所有私网 IPv6 地址的路由。

PE 1 在 Ping 远端 CE 网段时，会使用当前设备上指定 VPN 实例中所有处于 UP 状态的接口的 IPv6 地址中，最小的 IPv6 地址作为 ICMPv6 报文的源地址，如果 CE 3 没有该 IPv6 地址的路由信息，将会导致 ICMPv6 报文无法返回。

上述问题可以通过以下方法解决：

- 在 PE 1 上配置发布本设备的所有私网路由，例如，在 BGP-VPN IPv6 单播地址族视图下，配置 **import-route direct** 命令。
- 执行 Ping 操作时，指定 ICMPv6 回显请求报文中的源 IPv6 地址为 CE 3 的 IPv6 路由表中存在的地址，即执行 **ping ipv6 -a** *source-ipv6* **-vpn-instance** *vpn-instance-name host* 命令。

如果故障仍不能排除，请执行步骤（2）。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11.4 MPLS TE故障处理

11.4.1 MPLS TE 隧道状态为 Down

1. 故障描述

完成 MPLS TE 隧道创建后，通过 **display interface tunnel** 命令查看到 MPLS TE 隧道的当前状态为 DOWN。

```
<Sysname> display interface tunnel 1
Tunnel1
Current state: DOWN
Line protocol state: DOWN
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1496
Internet address: 7.1.1.1/24 (primary)
Tunnel source unknown, destination 4.4.4.9
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 6 bytes/sec, 48 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 177 packets, 11428 bytes, 0 drops
```

2. 常见原因

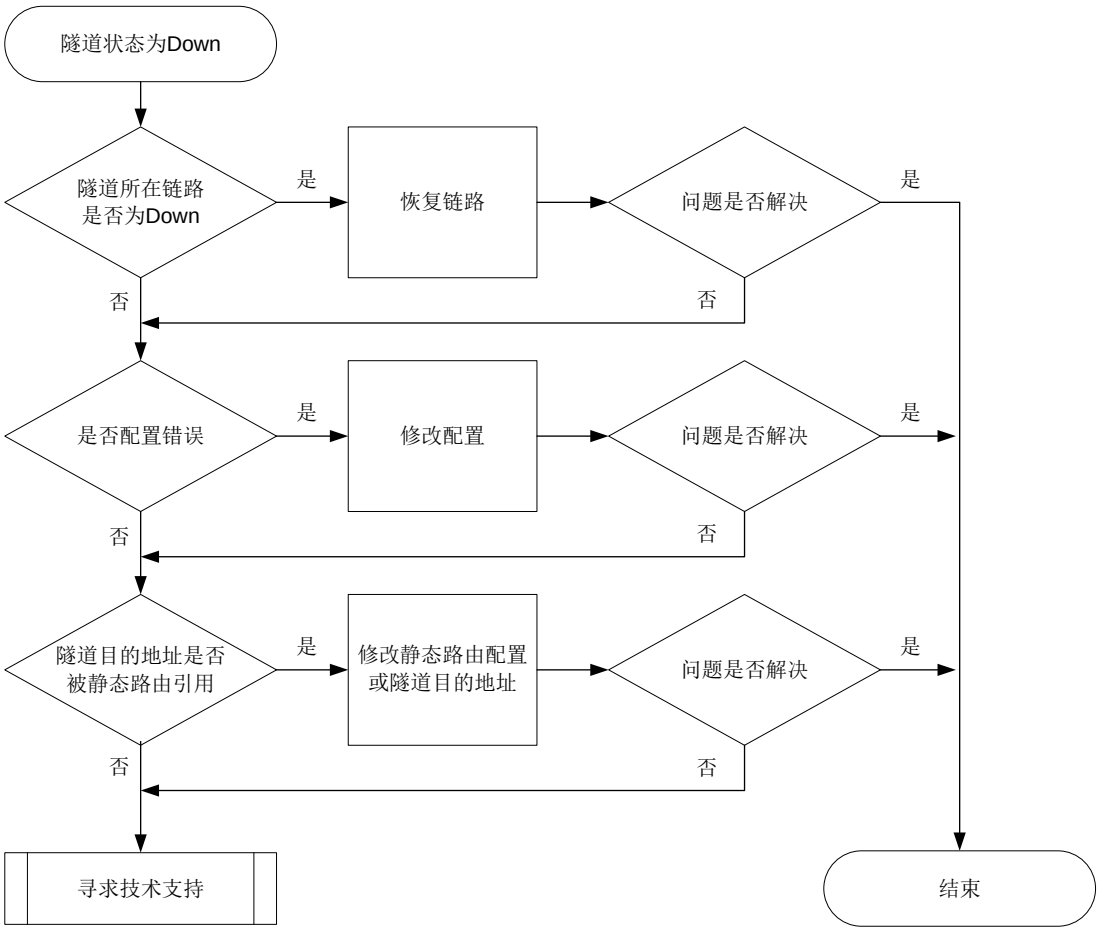
本类故障的常见原因主要包括：

- MPLS TE 隧道所在的链路 Down。
- MPLS TE 配置错误。
- MPLS TE 隧道的目的地址被静态路由引用。

3. 故障分析

本类故障的诊断流程如图 76 所示。

图76 MPLS TE 隧道状态为 Down 的故障诊断流程图



4. 处理步骤

(1) 查看 MPLS TE 隧道对应的接口是否为 Up 状态。

执行 **display interface** 命令，查看 MPLS TE 隧道对应的接口否为 Up 状态。

(2) 检查 MPLS TE 配置。

依次检查如下配置：

a. OSPF/IS-IS 区域和 MPLS TE 隧道经过的接口下是否配置 **mpls te enable** 命令。

b. LSR ID、Router ID 是否为同一 LoopBack 接口的地址。

c. 若使用 RSVP-TE 协议建立 MPLS TE 隧道，则需要检查设备和接口是否配置了 **rsvp**、**rsvp enable** 命令。

d. 若隧道接口下配置了 **mpls te bandwidth** 命令，检查设备出接口是否配置了 **mpls te max-link-bandwidth** 以及 **mpls te max-reservable-bandwidth** 命令。

e. 若隧道接口下配置了 **mpls te affinity-attribute** 命令，检查设备出接口是否配置合理的 **mpls te link-attribute** 命令。如果希望某条链路能够被隧道所用，则需要满足如下要求：

– 对于隧道亲和属性掩码为 1 的位，亲和属性为 1 的位中链路属性至少有 1 位也为 1，亲和属性为 0 的位对应的链路属性位不能为 1。

– 对于隧道亲和属性掩码为 0 的位，不对链路属性的相应位进行检查。

f. 若使用 Segment Routing 协议建立 MPLS TE 隧道，则需要检查设备 IGP 区域下是否配置了 Segment-Routing 相关功能。

g. 若使用 **mpls te path** 命令指定显式路径来建立 MPLS TE 隧道，则需要检查显式路径配置是否合理：使用 strict 方式时，需要逐跳指定入接口的 IP 地址；使用 loose 方式时，需要指定经过的设备的节点地址。

(3) 查看 MPLS TE 隧道的目的地址是否被静态引用。

执行 **display current-configuration | include** *destination* 命令，查看 MPLS TE 隧道的目的地址是否被静态引用。如果被静态路由引用，则需要根据用户的实际组网需求修改静态路由或者隧道的目的地址。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

无

11.4.2 MPLS TE 隧道由 UP 状态变为 Down 状态

1. 故障描述

MPLS TE 隧道由 UP 状态变为 Down 状态。

2. 常见原因

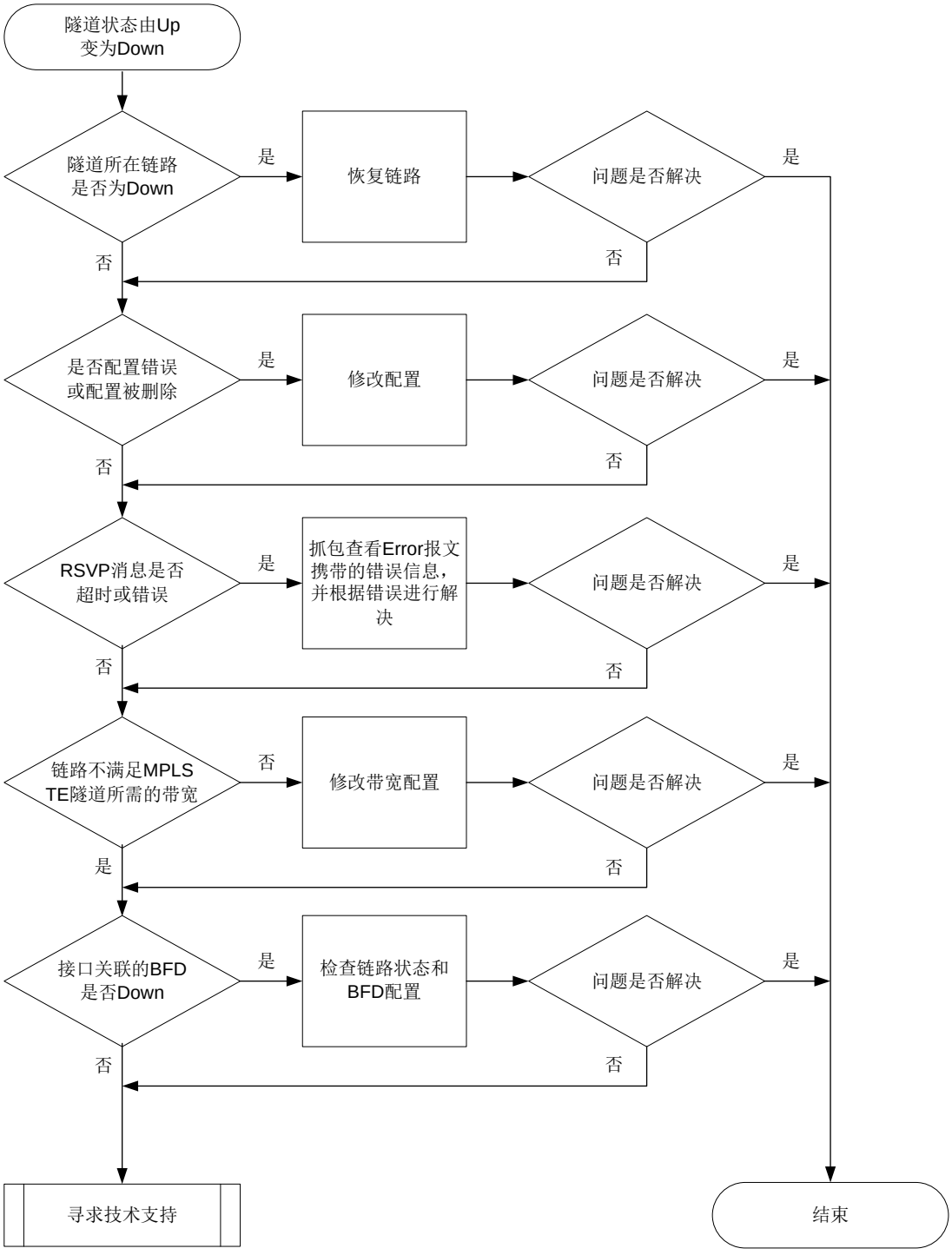
本类故障的常见原因主要包括：

- MPLS TE 隧道所在的链路 Down。
- MPLS TE 隧道的配置被删除或配置错误。
- RSVP 消息超时或错误。
- 物理链路不满足 MPLS TE 隧道所需的带宽。
- MPLS TE 隧道或隧道所在物理接口 BFD down。

3. 故障分析

本类故障的诊断流程如图图 77所示。

图77 MPLS TE 隧道由 UP 状态突然变为 Down 状态的故障诊断流程图



4. 处理步骤

(1) 查看 MPLS TE 隧道对应的接口是否为 Up 状态。

执行 **display interface** 命令，查看 MPLS TE 隧道对应的接口否为 Up 状态。

(2) 检查 MPLS TE 配置。

依次检查如下配置：

a. OSPF/IS-IS 区域和 MPLS TE 隧道经过的接口下是否配置 **mpls te enable** 命令。

b. LSR ID、Router ID 是否为同一 LoopBack 接口的地址。

c. 若使用 RSVP-TE 协议建立 MPLS TE 隧道，则需要检查设备和接口是否配置了 **rsvp**、**rsvp enable** 命令。

d. 若隧道接口下配置了 **mpls te bandwidth** 命令，检查设备出接口是否配置了 **mpls te max-link bandwidth** 以及 **mpls te max-reservable bandwidth** 命令。

e. 若隧道接口下配置了 **mpls te affinity-attribute** 命令，检查设备出接口是否配置合理的 **mpls te link-attribute** 命令。如果希望某条链路能够被隧道所用，则需要满足如下要求：

   – 对于隧道亲和属性掩码为 1 的位，亲和属性为 1 的位中链路属性至少有 1 位也为 1，亲和属性为 0 的位对应的链路属性位不能为 1。

   – 对于隧道亲和属性掩码为 0 的位，不对链路属性的相应位进行检查。

f. 若使用 Segment Routing 协议建立 MPLS TE 隧道，则需要检查设备 IGP 区域下是否配置了 Segment-Routing 相关功能。

g. 若使用 **mpls te path** 命令指定显式路径来建立 MPLS TE 隧道，则需要检查显式路径配置是否合理：使用 strict 方式时，需要逐跳指定入接口的 IP 地址；使用 loose 方式时，需要指定经过的设备的节点地址。

(3) 检查是否存在 RSVP 消息超时或错误。

通过 **display rsvp statistics** 命令查看是否存在 RSVP 消息超时（即发送的 Path 消息和收到的 Resv 消息个数不一致、收到的 Path 消息和发送的 Resv 消息个数不一致）或 RSVP 消息错误（即收到 PathError 消息或 ResvError 消息）的问题。若存在 RSVP 消息超时或错误，请抓包查看 PathError 消息或 ResvError 报文携带的错误信息，并根据报文携带的错误码，参照 RFC 2205 和 RFC 3209 解决问题。

```
<Sysname> display rsvp statistics
P2P statistics:
Object                  Added             Deleted
  PSB                   3                 1
  RSB                   3                 1
  LSP                   3                 1
P2MP statistics:
Object                  Added             Deleted
  PSB                   0                 0
  RSB                   0                 0
  LSP                   0                 0

Packet                  Received          Sent
  Path                  5                 5
  Resv                  5                 5
  PathError             0                 0
  ResvError             0                 0
  PathTear              0                 0
  ResvTear              0                 0
  ResvConf              0                 0
  Bundle                0                 0
```

```
Ack                 0                   0
Srefresh            0                   0
Hello               0                   0
Challenge           0                   0
Response            0                   0
Error               0                   0
```

(4) 检查物理链路是否满足 MPLS TE 隧道所需的带宽。

当设备上建立了更高优先级的 MPLS TE 隧道时，该隧道可能会抢占低优先级 MPLS TE 隧道的带宽，导致低优先级 MPLS TE 隧道的状态变为 down。通过 **display mpls te link-management bandwidth-allocation** 命令查看链路上各个优先级的剩余可用带宽，确保链路剩余可用带宽大于该优先级的隧道所需的带宽。如果链路上的剩余可用带宽不能满足 MPLS TE 隧道的需求，则需要修改配置，调整隧道路径，或为链路提供更大的带宽。

(5) 检查 MPLS TE 隧道或隧道所在物理接口是否 BFD down。

通过 **display mpls bfd te tunnel** *tunnel-number* 命令查看 MPLS TE 隧道的 BFD 状态。若 MPLS TE 隧道的 BFD 状态为 down，则需要通过 **display bfd session** 命令查看 BFD 状态为 down 的原因，检查并修改 BFD 配置或检查物理链路是否存在链路故障、链路质量问题。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：MPLS-TE-STD-MIB

- mplsTunnelUp (1.3.6.1.2.1.10.166.3.0.1)
- mplsTunnelDown (11.3.6.1.2.1.10.166.3.0.2)

相关日志

- IFNET/5/LINK_UPDOWN
- IFNET/3/PHY_UPDOWN

11.4.3 MPLS TE 隧道存在环路

1. 故障描述

MPLS TE 隧道的转发路径上存在环路，导致流量无法通过 MPLS TE 隧道转发到目的地址。

2. 常见原因

MPLS TE 隧道经过的不同设备上存在相同的 IP 地址。

3. 处理步骤

(1) 请检查 MPLS TE 隧道经过的不同设备上是否配置了相同的 IP 地址。若存在相同的 IP 地址，则需要修改 IP 地址，保证 MPLS TE 隧道经过的不同设备上不存在相同的 IP 地址。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。

- 设备的配置文件。
- 使用 **display diagnostic-information** 命令收集诊断信息。

4. 告警与日志

相关告警

无

相关日志

无

11.4.4 Tunnel 路径计算失败

1. 故障描述

MPLS TE 隧道路径计算失败，导致隧道 DOWN。

2. 常见原因

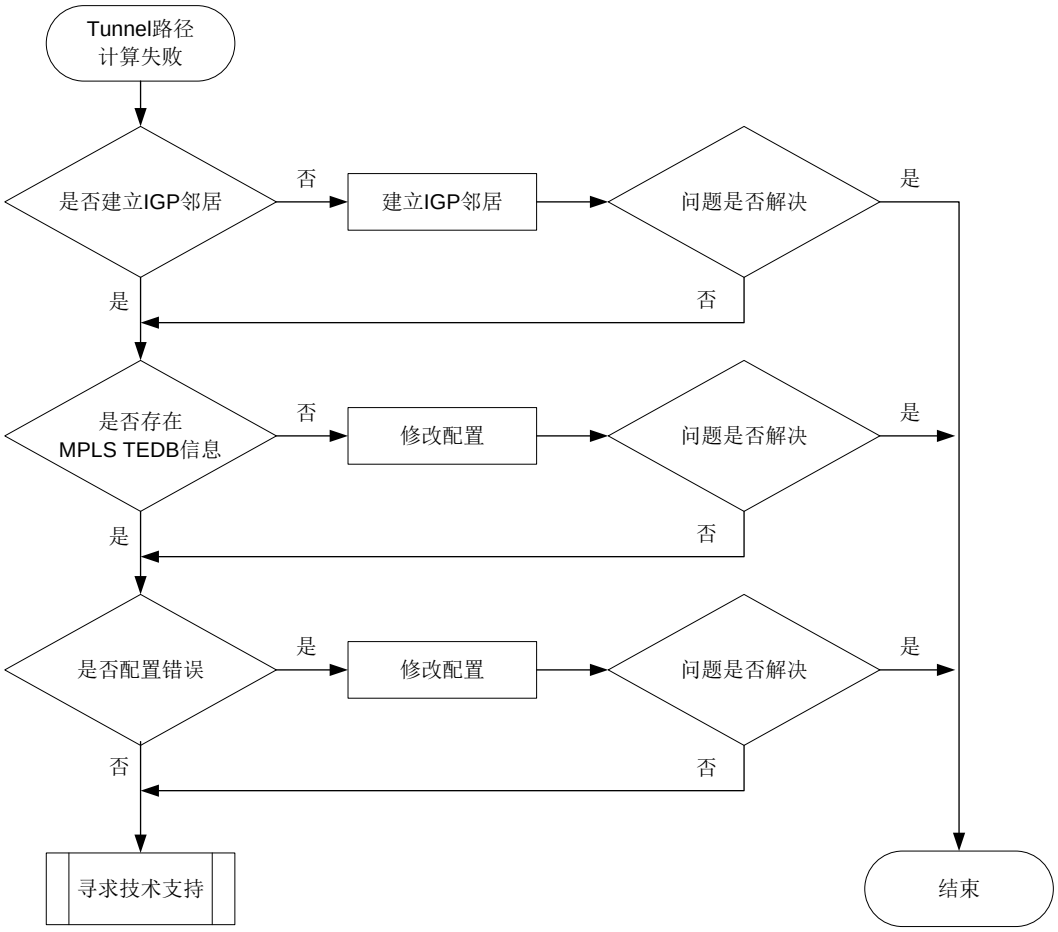
本类故障的常见原因主要包括：

- 没有建立 IGP 邻居。
- 没有 MPLS TEDB 信息。
- MPLS TE 配置错误。

3. 故障分析

本类故障的诊断流程如图 78 所示。

图78 Tunnel 路径计算失败的故障诊断流程图



4. 处理步骤

(1) 查看是否建立了 IGP 邻居。

执行 **display ospf peer** 和 **display isis peer** 命令，查看是否建立了 IGP 邻居。

- 若建立了 IGP 邻居，请继续执行第(2)步。
- 若没有建立了 IGP 邻居，请先完成 OSPF 或 IS-IS 配置，建立 IGP 邻居。OSPF 的详细介绍，请参见“三层技术-IP 路由”中的“OSPF”；IS-IS 的详细介绍，请参见“三层技术-IP 路由”中的“IS-IS”。

(2) 执行 **display mpls te tedb** 命令，查看 MPLS TEDB 信息。

若存在 MPLS TEDB 信息，请继续执行第(3)步。

若不存在 MPLS TEDB 信息，请依次检查如下配置：

a. OSPF/IS-IS 区域和 MPLS TE 隧道经过的接口下是否配置 **mpls enable**、**mpls te enable** 命令。

b. LSR ID、Router ID 是否为同一 LoopBack 接口的地址。

(3) 检查 MPLS TE 配置。

a. 若使用 RSVP-TE 协议建立 MPLS TE 隧道，则需要检查设备和接口是否配置了 **rsvp**、**rsvp enable** 命令。

b. 若使用 Segment Routing 协议建立 MPLS TE 隧道，则需要检查设备 IGP 区域下是否配置了 **segment-routing mpls** 命令。

c. 若隧道接口下配置了 **mpls te bandwidth** 命令，检查设备出接口是否配置了 **mpls te max-link-bandwidth** 以及 **mpls te max-reservable-bandwidth** 命令。

d. 若隧道接口下配置了 **mpls te affinity-attribute** 命令，检查设备出接口是否配置合理的 **mpls te link-attribute** 命令。如果希望某条链路能够被隧道所用，则需要满足如下要求：

   – 对于隧道亲和属性掩码为 1 的位，亲和属性为 1 的位中链路属性至少有 1 位也为 1，亲和属性为 0 的位对应的链路属性位不能为 1。

   – 对于隧道亲和属性掩码为 0 的位，链路属性可以是任意值。

e. 若使用 **mpls te path** 命令指定显式路径来建立 MPLS TE 隧道，则需要检查显式路径配置是否合理：使用 strict 方式时，需要逐跳指定入接口的 IP 地址；使用 loose 方式时，需要指定经过的设备的节点地址。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

无

11.4.5 热备份 CRLSP 无法建立

1. 故障描述

MPLS TE 隧道下配置 **mpls te backup hot-standby** 命令，但是无法建立备份 CRLSP。

2. 常见原因

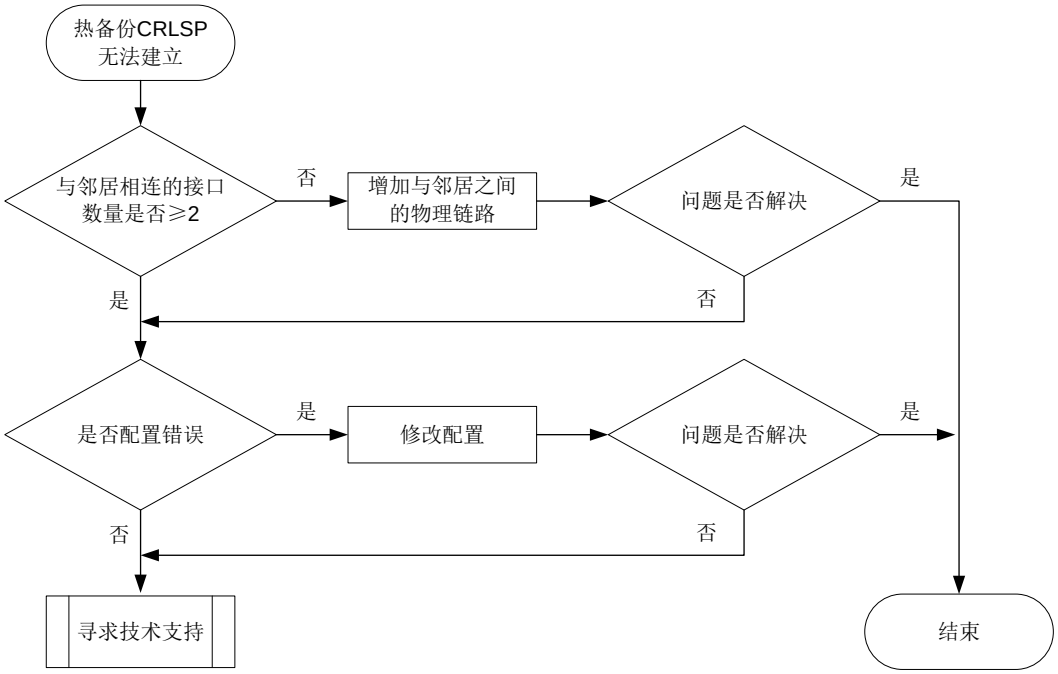
本类故障的常见原因主要包括：

- 只存在一个与邻居相邻的接口。
- MPLS TE 配置错误。

3. 故障分析

本类故障的诊断流程如图 79 所示。

图79 热备份 CRLSP 无法建立的故障诊断流程图



4. 处理步骤

(1) 根据配置的 IGP 协议，执行 **display ospf peer** 或 **display isis peer** 命令，查看与同一邻居（同一 System ID 或同一 Router ID）相连的接口信息（interface）。

显示 IS-IS 邻居的概要信息。

```
<Sysname> display isis peer

                    Peer information for IS-IS(1)
                    ----------------------------

 System ID: 0000.0000.0001
 Interface: GE1/0/1                Circuit Id:  0000.0000.0001.01
 State: Up     HoldTime:  27s      Type: L1(L1L2)     PRI: 64

 System ID: 0000.0000.0001
 Interface: GE1/0/2                Circuit Id:  0000.0000.0001.01
 State: Up     HoldTime:  27s      Type: L2(L1L2)     PRI: 64
```

显示 OSPF 邻居概要信息。

```
<Sysname> display ospf peer

          OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 1.1.1.2         1.1.1.2         1   40         Full/DR           GE1/0/1
```

- 若与邻居相连的接口数量≥2，请继续执行第(2)步。
- 若与邻居相连的接口数量＜2，请增加与邻居之间的物理链路，确保存在可以建立备份 CRLSP 的路径。

(2) 检查 MPLS TE 配置。

依次检查如下配置：

a. OSPF/IS-IS 区域和 MPLS TE 隧道经过的接口下是否配置 **mpls te enable** 命令。

b. LSR ID、Router ID 是否为同一 LoopBack 接口的地址。

c. 若使用 RSVP-TE 协议建立 MPLS TE 隧道，则需要检查设备和接口是否配置了 **rsvp**、**rsvp enable** 命令。

d. 若隧道接口下配置了 **mpls te bandwidth** 命令，检查设备出接口是否配置了 **mpls te max-link-bandwidth** 以及 **mpls te max-reservable-bandwidth** 命令。

e. 若隧道接口下配置了 **mpls te affinity-attribute** 命令，检查设备出接口是否配置合理的 **mpls te link-attribute** 命令。如果希望某条链路能够被隧道所用，则需要满足如下要求：

   – 对于隧道亲和属性掩码为 1 的位，亲和属性为 1 的位中链路属性至少有 1 位也为 1，亲和属性为 0 的位对应的链路属性位不能为 1。

   – 对于隧道亲和属性掩码为 0 的位，链路属性可以是任意值。

f. 若使用 Segment Routing 协议建立 MPLS TE 隧道，则需要检查设备 IGP 区域下是否配置了 **segment-routing mpls** 命令。

g. 若使用 **mpls te path** 命令指定显式路径来建立 MPLS TE 隧道，则需要检查显式路径配置是否合理：使用 strict 方式时，需要逐跳指定入接口的 IP 地址；使用 loose 方式时，需要指定经过的设备的节点地址。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

- TE/5/TE_BACKUP_SWITCH

11.5 MPLS基础故障处理

11.5.1 报文通过 LSP 隧道转发不通

1. 故障描述

网络中主机的发送报文，通过 LSP 隧道转发不通。

2. 常见原因

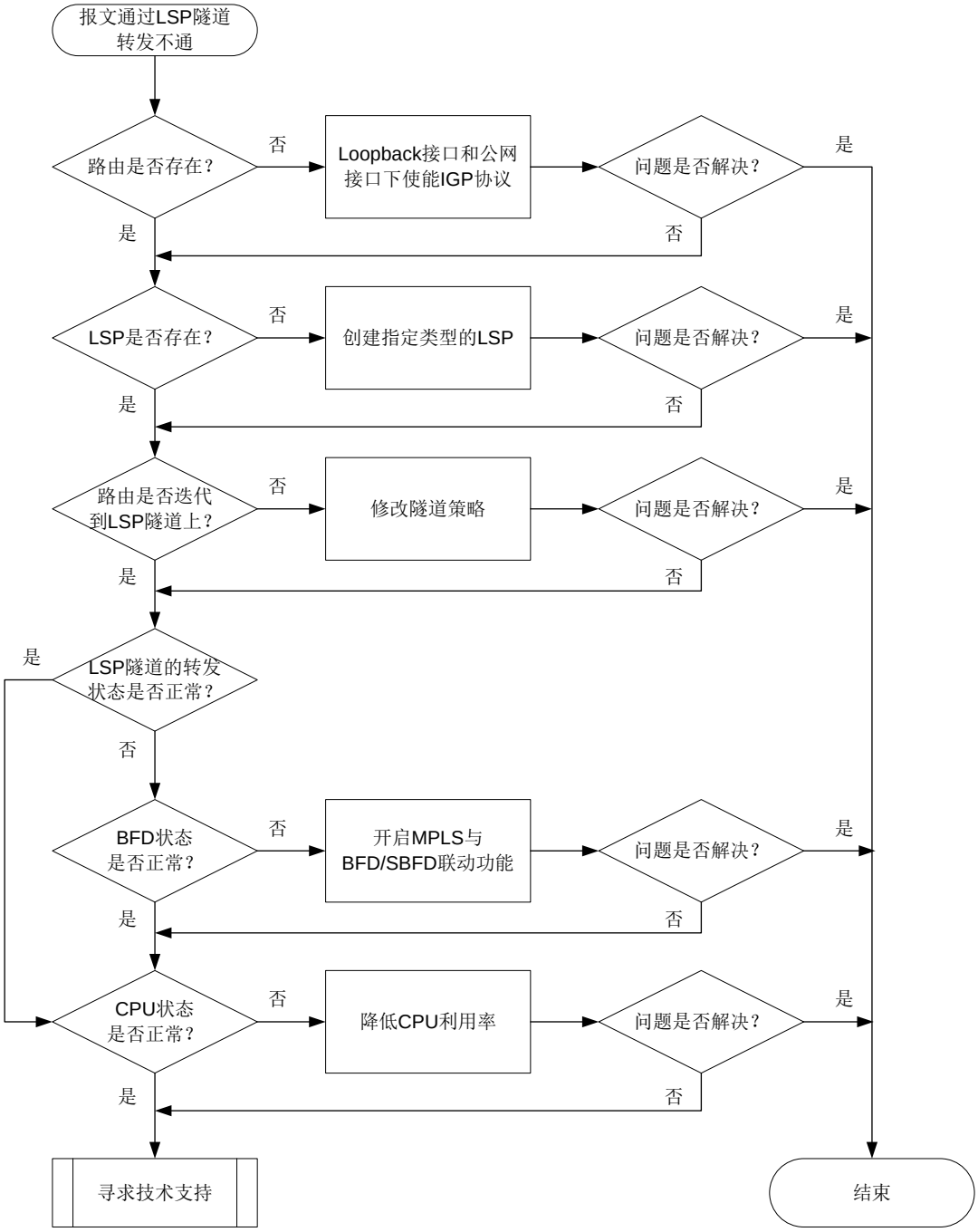
本类故障的常见原因主要包括：

- 路由不存在。
- LSP 不存在。
- 路由未迭代到 LSP 隧道上。
- LSP 隧道的转发状态非 ACTIVE。
- BFD 会话状态为 Down。
- CPU 利用率过高。

3. 故障分析

本类故障的诊断流程如图 80 所示。

图80 报文通过 LSP 隧道转发不通的故障诊断流程图



4. 处理步骤

(1) 检查 IGP 路由是否存在。

执行 **display ip routing-table** 命令，查看是否存在到达目的节点的 Loopback 接口地址的网段路由：

```
<Sysname> display ip routing-table 1.1.1.1

Summary count : 1
```

```
Destination/Mask   Proto   Pre Cost        NextHop         Interface
1.1.1.2/32         IS_L1   15  10          1.1.1.1         LoopBack1
```

- 如果不存在，则在 Loopback 接口和公网接口下使能 IGP 协议，确保发布对应网段路由。
- 如果存在，则执行步骤(2)。

(2) 检查 LSP 是否存在。

执行 **display mpls lsp** 命令，查看是否存在到达目的节点的 Loopback 接口的 LSP：

- 如果不存在，则确保建立指定类型的 LSP：
  - 对于 LDP LSP，请在接口下使能 MPLS 功能和 MPLS LDP 功能。
  - 对于 SRLSP，请在 IS-IS IPv4 单播地址族视图、OSPF 视图或 BGP IPv4 单播地址族视图下执行 **segment-routing mpls** 命令用来开启基于 MPLS 的 SR 功能。
  - 对于 SR-MPLS TE Policy，请在 SR-TE 视图下创建正确的 SR-MPLS TE Policy。
- 如果存在，则执行步骤(3)。

```
<Sysname> display mpls lsp
FEC                         Proto    In/Out Label    Out Inter/NHLFE/LSINDEX
1.1.1.2/32                  LDP      -/1049          GE1/0/1
```

(3) 检查路由是否迭代到 LSP 隧道上。

执行 **display mpls tunnel all** 命令，查看所有隧道的信息。执行 **display fib** 命令，查看指定下一跳地址的 FIB 表项。对于 FIB 表项中 Nexthop 字段与隧道信息中 Destination 字段相同值的 FIB 表项，检查该 FIB 表项的 LSP 索引号（Token 字段）与隧道的 NHLFE ID 是否相同。

- 如果不同，则表示未迭代到 LSP 隧道上，确认指定 FEC 的隧道类型（Type 字段）与配置的隧道策略是否相同：
  - 如果不同，则在隧道策略视图下修改隧道策略，使配置的隧道策略与指定 FEC 的隧道类型匹配。
  - 如果相同，则执行步骤(7)。

```
<Sysname> display tunnel-policy
Tunnel policy name: abc
  Select-Seq: LSP
    Load balance number   : 1
    Strict                : No
```

- 如果相同，则表示迭代到 LSP 隧道上，请执行步骤(4)。

```
<Sysname> display mpls tunnel all
Destination      Type     Tunnel/NHLFE      VPN Instance
2.2.2.9          LSP      NHLFE3            -
3.3.3.9          SRLSP    NHLFE2            -
4.4.4.9          SRPolicy NHLFE23068673     -
<Sysname> display fib
Destination count: 1 FIB entry count: 1
Flag:
  U:Usable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay    F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
55.55.55.55/32     2.2.2.9         UGHR     3                        Null
```

…

(4) 检查 LSP 隧道的转发状态是否正常。

执行 **display mpls forwarding nhlfe** 命令，查看指定 NHLFE 表项信息。

- 如果转发标记中没有 A 标记，则表示该 LSP 隧道无法使用，请执行步骤(5)。
- 如果转发标记中有 A 标记，则表示该 LSP 隧道可以正常使用，请执行步骤(6)。

```
<Sysname> display mpls forwarding  nhlfe  3
Flags: T - Forwarded through a tunnel
       N - Forwarded through the outgoing interface to the nexthop IP address
       B - Backup forwarding information
       A - Active forwarding information
       M - P2MP forwarding information
       S - Secondary backup path

NID        Tnl-Type   Flag OutLabel Forwarding Info
------------------------------------------------------------------------------
3          LSP        NA   1040127  GE1/0/3                 10.0.3.2
```

(5) 检查 BFD 状态是否正常。

执行 **display mpls bfd** 命令或 **display mpls sbfd** 命令，查看 LSP 隧道的 BFD/SBFD 检测信息：

- 如果 BFD/SBFD 会话状态显示为 Down，则在系统视图下执行 **mpls bfd enable** 命令开启 MPLS 与 BFD/SBFD 联动功能，确保检测 LSP 隧道的 BFD/SBFD 会话 Up。
- 如果 BFD/SBFD 会话状态显示为 Up，则执行步骤(6)。

```
<Sysname> display mpls bfd ipv4 22.22.2.2 32
 Total number of sessions: 1, 1 up, 0 down, 0 init

 FEC Type: LSP
 FEC Info:
   Destination: 22.22.2.2
   Mask Length: 32
 NHLFE ID: 1025
 Local Discr: 513                    Remote Discr: 513
 Source IP: 11.11.1.1                Destination IP: 127.0.0.1
 Session State: Up                   Session Role: Passive
 Template Name: -
<Sysname> display mpls sbfd ipv4 22.22.2.2 32
 Total number of sessions: 1, 1 up, 0 down, 0 init

 FEC Type: LSP
 FEC Info:
   Destination: 22.22.2.2
   Mask Length: 32
 NHLFE ID: 1025
 Local Discr: 513                    Remote Discr: 513
 Source IP: 11.11.1.1                Destination IP: 127.0.0.1
 Session State: Up
 Template Name: -
```

(6) 检查 CPU 状态是否正常。

执行 **display cpu-usage** 命令，查看 CPU 利用率的统计信息。

- 如果 CPU 利用率过高，则关闭一些不必要的功能，降低设备 CPU 利用率。
- 如果 CPU 利用率正常，则执行步骤(7)。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

11.6 VPLS故障处理

11.6.1 PW 两端的 PE 设备中只有一个 PE 上的 VSI 处于 Up 状态

1. 故障描述

PW 两端的 PE 设备中只有一个 PE 上的 VSI 处于 Up 状态。

2. 常见原因

VSI up 的条件为：

- VSI 下至少有一个 PW Up 和一个 AC up。
- VSI 下至少有两个 AC Up。

因此本类故障的常见原因为：Up 的 VSI 上虽然 PW down，但是存在两个 Up 的 AC；Down 的 VSI 上 PW down，且无两个 Up 的 AC。

3. 故障分析

本类故障的诊断思路为：检查状态为 Down 的 VSI 下的 AC 和 PW 的状态。

4. 处理步骤

(1) 执行 **display l2vpn vsi** 命令，查看 VSI 下 AC 和 PW 的状态。

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpls1
  VSI Index               : 0
  VSI Description         : vsi for vpls1
  VSI State               : Down
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
```

```
  MAC Learning rate       : -
  Drop Unknown            : -
  PW Redundancy           : Master
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : -
  LDP PWs:
    Peer            PW ID           Link ID    State
    192.3.3.3       1               8          Down
  ACs:
    AC                              Link ID    State       Type
    GE1/0/3 srv1                    1          Up          Manual
```

(2) 执行 **display l2vpn pw verbose** 命令，查看 PW 状态变为 Down 的原因。

```
<Sysname> display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          Remote Site: 2
    Signaling Protocol  : BGP
    Link ID             : 9          PW State : Down
    In Label            : 1420       Out Label: 1419
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Flow Label          : Send
    Control Word        : Disabled
    Tunnel Group ID     : 0x800000960000000
    Tunnel NHLFE IDs    : 1038
    Admin PW            : -
    E-Tree Mode         : -
    E-Tree Role         : root
    Root VLAN           : -
    Leaf VLAN           : -
    Down Reasons        : Control word not match
```

常见的故障原因及处理方法如下：

- BFD session for PW down：用来检测 PW 的 BFD 会话状态为 down，此类故障的处理方式为，通过 **display bfd session** 命令查看 BFD 状态为 down 的原因，检查并修改 BFD 配置或检查物理链路是否存在链路故障、链路质量问题。
- BGP RD was deleted：BGP 的 RD 被删除，此类故障的处理方式为，在交叉连接组自动发现视图下配置 **route-distinguisher** *route-distinguisher* 命令。
- BGP RD was empty：未配置 BGP 的 RD，此类故障的处理方式为，在交叉连接组自动发现视图下配置 **route-distinguisher** *route-distinguisher* 命令。
- Control word not match：PW 两端控制字功能配置不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的控制字功能（通过 **control-word enable** 命令开启）配置一致。
- Encapsulation not match：PW 两端封装类型不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的 PW 数据封装类型（通过 **pw-type** 命令配置）配置一致。

- LDP interface parameter not match：PW 两端接口 LDP 协商参数不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的 VCCV 控制通道类型（通过 **vccv cc** 命令配置）配置一致或将 PW 两端关联的电路仿真接口下引用的电路仿真类中的配置保持一致。
- Non-existent remote LDP PW：对端设备已删除 LDP PW，此类故障的处理方式为，在对端设备上重新配置 PW。
- Local AC Down：本地 AC 状态为 down，此类故障的处理方式为，检查并修改 AC 接口上的配置或排除 AC 所在的接口的故障，保障接口为 Up 状态。
- Local AC was non-existent：未配置本地 AC，此类故障的处理方式为，配置本地的 AC 并关联 VSI。
- MTU not match：PW 两端 MTU 不一致，此类故障的处理方式为，将 PW 两端的 MTU 配置一致或者通过 **mtu-negotiate disable** 命令关闭 PW MTU 协商功能。
- Remote AC Down：对端 AC 状态 down，此类故障的处理方式为，检查并修改对端 AC 接口上的配置或排除 AC 所在的接口的故障，保障接口为 Up 状态。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

- L2VPN/2/L2VPN_PWSTATE_CHANGE
- L2VPN/4/L2VPN_BGPVC_CONFLICT_LOCAL
- L2VPN/4/L2VPN_BGPVC_CONFLICT_REMOTE
- L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH
- L2VPN/2/L2VPN_HARD_RESOURCE_RESTORE
- L2VPN/4/L2VPN_LABEL_DUPLICATE

11.6.2 VPLS 业务不通

1. 故障描述

VPLS 业务流量转发不通。

2. 常见原因

本类故障的常见原因主要包括：

- AC 没有 Up
- PW 没有 Up。
- PW 没有生成转发信息。
- PW 没有可迭代的公网隧道。
- PW 迭代的公网隧道异常。

3. 故障分析

本类故障的诊断思路如下：

(1) 查看 VSI 详细信息，确认 VSI 下至少关联了一个 AC 和一个 PW。

(2) 检查 AC 状态是否 Up。

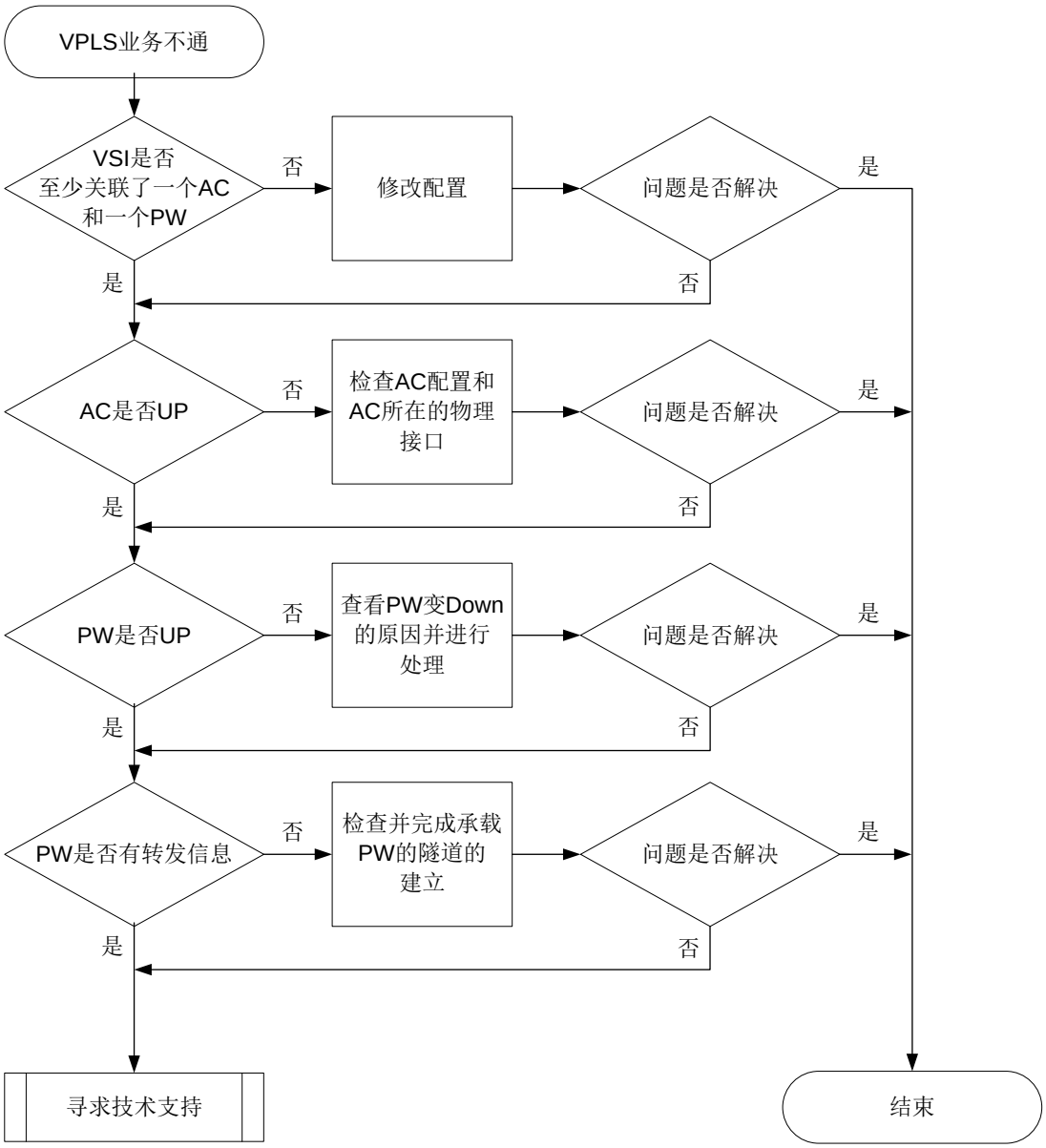
(3) 检查 PW 状态是否 Up。

(4) 检查 PW 转发信息。

(5) 检查 PW 迭代的公网隧道信息。

本类故障的诊断流程如图 81 所示。

图81 VPLS 业务不通的故障诊断流程图



4. 处理步骤

(1) 执行 **display l2vpn vsi** 命令，查看 VSI 关联的 AC、PW 的状态和数量。

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpls1
  VSI Index               : 0
  VSI Description         : vsi for vpls1
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  PW Redundancy           : Master
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : -
  LDP PWs:
    Peer            PW ID            Link ID    State
    192.3.3.3       1                8          Down
  ACs:
    AC                               Link ID    State       Type
    GE1/0/3 srv1                     1          Up          Manual
```

(2) 若 AC 的状态为 Down，则检查 AC 配置是否正确和并检查 AC 所在的接口是否 Up。如果 AC 配置不正确或 AC 所在的接口为 Down 状态，请修改 AC 配置或排查接口故障。

(3) 若 PW 的状态为 Down，请通过 **display l2vpn pw verbose** 命令查看 PW 状态变为 Down 的原因。

```
<Sysname> display l2vpn pw verbose
VSI Name: aaa
  Peer: 2.2.2.9          Remote Site: 2
    Signaling Protocol  : BGP
    Link ID             : 9          PW State : Down
    In Label            : 1420       Out Label: 1419
    MTU                 : 1500
    PW Attributes       : Main
    VCCV CC             : -
    VCCV BFD            : -
    Flow Label          : Send
    Control Word        : Disabled
    Tunnel Group ID     : 0x800000960000000
    Tunnel NHLFE IDs    : 1038
    Admin PW            : -
    E-Tree Mode         : -
    E-Tree Role         : root
    Root VLAN           : -
    Leaf VLAN           : -
    Down Reasons        : Control word not match
```

常见的故障原因及处理方法如下：

- BFD session for PW down：用来检测 PW 的 BFD 会话状态为 down，此类故障的处理方式为，通过 **display bfd session** 命令查看 BFD 状态为 down 的原因，检查并修改 BFD 配置或检查物理链路是否存在链路故障、链路质量问题。
- BGP RD was deleted：BGP 的 RD 被删除，此类故障的处理方式为，在交叉连接组自动发现视图下配置 **route-distinguisher** *route-distinguisher* 命令。
- BGP RD was empty：未配置 BGP 的 RD，此类故障的处理方式为，在交叉连接组自动发现视图下配置 **route-distinguisher** *route-distinguisher* 命令。
- Control word not match：PW 两端控制字功能配置不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的控制字功能（通过 **control-word enable** 命令开启）配置一致。
- Encapsulation not match：PW 两端封装类型不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的 PW 数据封装类型（通过 **pw-type** 命令配置）配置一致。
- LDP interface parameter not match：PW 两端接口 LDP 协商参数不一致，此类故障的处理方式为，将 PW 两端引用的 PW 模板下的 VCCV 控制通道类型（通过 **vccv cc** 命令配置）配置一致或将 PW 两端关联的电路仿真接口下引用的电路仿真类中的配置保持一致。
- Non-existent remote LDP PW：对端设备已删除 LDP PW，此类故障的处理方式为，在对端设备上重新配置 PW。
- Local AC Down：本地 AC 状态为 down，此类故障的处理方式为，检查并修改 AC 接口上的配置或排除 AC 所在的接口的故障，保障接口为 Up 状态。
- Local AC was non-existent：未配置本地 AC，此类故障的处理方式为，配置本地的 AC 并关联 VSI。
- MTU not match：PW 两端 MTU 不一致，此类故障的处理方式为，将 PW 两端的 MTU 配置一致或者通过 **mtu-negotiate disable** 命令关闭 PW MTU 协商功能。
- Remote AC Down：对端 AC 状态 down，此类故障的处理方式为，检查并修改对端 AC 接口上的配置或排除 AC 所在的接口的故障，保障接口为 Up 状态。

(4) 若 AC 和 PW 均处于 Up 状态，请通过 **display l2vpn forwarding pw verbose** 命令查看 PW 是否存在转发信息，即承载 PW 的隧道对应的 NHLFE 表项索引列表（Tunnel NHLFE IDs）。

- 如果存在转发信息，请执行步骤(6)。
- 如果不存在转发信息，请执行步骤(5)。

```
<Sysname> display l2vpn forwarding pw verbose
VSI Name: aaa
  Link ID: 8
    PW Type          : VLAN                  PW State : Up
    In Label         : 1272                  Out Label: 1275
    MTU              : 1500
    PW Attributes    : Main
    VCCV CC          : Router-Alert
    VCCV BFD         : Fault Detection with BFD
    Flow Label       : Send
    Tunnel Group ID  : 0x960000000
    Tunnel NHLFE IDs: 1034
```

```
    MAC limit       : maximum=2000   alarm=enabled   action=discard
```

(5) 执行 **display mpls lsp** 命令，查看是否存在承载 PW 的隧道，即是否存在 FEC 为 PW 对端 IP 地址的 LSP，若不存在，则需要先完成承载 PW 的隧道的建立。

```
<Sysname> display mpls lsp
FEC                         Proto    In/Out Label    Out Inter/NHLFE/LSINDEX
100.100.100.100/24          LDP      -/1049          GE1/0/1
```

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

- L2VPN/2/L2VPN_PWSTATE_CHANGE
- L2VPN/4/L2VPN_BGPVC_CONFLICT_LOCAL
- L2VPN/4/L2VPN_BGPVC_CONFLICT_REMOTE
- L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH
- L2VPN/2/L2VPN_HARD_RESOURCE_RESTORE
- L2VPN/4/L2VPN_LABEL_DUPLICATE

11.6.3 PW 处于 Up 状态时两个 PE 间报文转发失败

1. 故障描述

PW 处于 Up 状态时两个 PE 间报文转发失败。

2. 常见原因

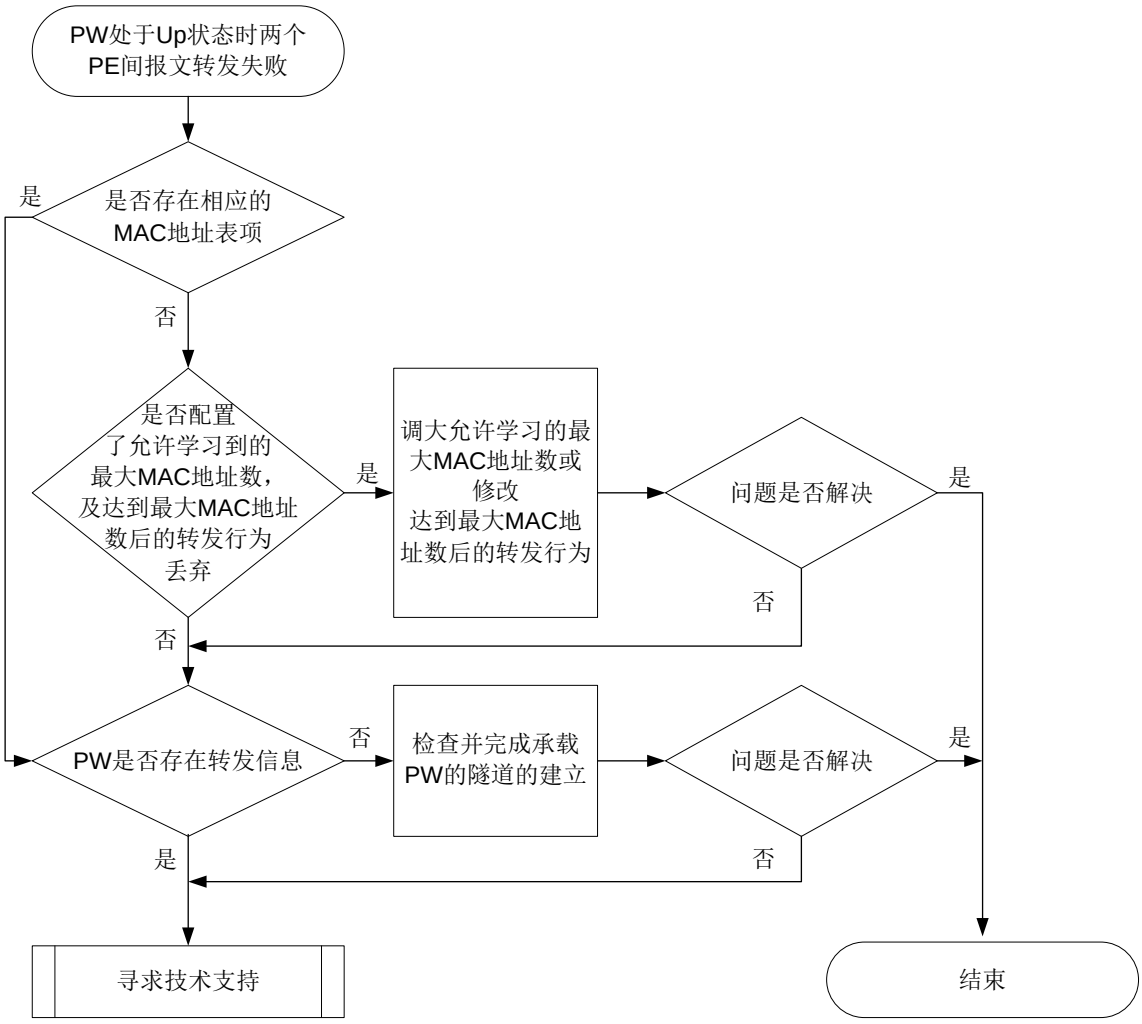
本类故障的常见原因主要包括：

- MAC 地址表达到允许 VSI 学习到的最大 MAC 地址数，并且配置当 VSI 学习到的 MAC 地址数达到最大值后，禁止转发源 MAC 地址不在 MAC 地址表里的报文，即丢弃该报文。
- PW 信息没有下发到转发模块。

3. 故障分析

本类故障的诊断流程如图 82 所示。

图82 PW 处于 Up 状态时两个 PE 间报文转发失败故障诊断流程图



4. 处理步骤

(1) 执行 **display l2vpn mac-address** 命令，查看是否存在相应的 MAC 地址表项和学习的 MAC 地址表项总数。可以通过指定具体的 AC 接口和 PW 信息，来显示从指定 AC 和 PW 上学习的 MAC 地址表项总数。

- 查看所有 L2VPN MAC 地址表项信息。

```
<Sysname> display l2vpn mac-address
* - The output interface is issued to another VSI
MAC Address    State     VSI Name                        Link ID/Name   Aging
0000-0000-000a Dynamic   vpn1                            GE1/0/1        Aging
0000-0000-0009 Dynamic   vpn1                            GE1/0/1        Aging
--- 2 mac address(es) found  ---
```

- # 显示 L2VPN MAC 地址表项总数。

```
<Sysname> display l2vpn mac-address count
2 mac address(es) found
```

(2) 查看是否配置了允许学习到的最大 MAC 地址数，及达到最大 MAC 地址数后的转发。

- 在 VSI 视图下执行 **display this** 命令，查看当前 VSI 下是否配置了 **mac-table limit** 命令和 **mac-table limit drop-unknown** 命令，如果配置了上述命令且当前已经学习到的 MAC 地址已经达到最大值，则需要将允许 VSI 学习到的最大 MAC 地址数调大或删除 **mac-table limit drop-unknown** 命令。
- 在 AC 和 PW 视图下执行 **display this** 命令，查看当前视图下是否配置了 **mac-limit** 命令，如果配置了该述命令且当前已经学习到的 MAC 地址已经达到最大值，则需要将允许学习到的最大 MAC 地址数调大或删除 **action discard** 参数。

(3) 执行 **display l2vpn forwarding pw verbose** 命令，查看 PW 是否存在转发信息，即承载 PW 的隧道对应的 NHLFE 表项索引列表（Tunnel NHLFE IDs）。

- 如果存在转发信息，请执行步骤(5)。
- 如果不存在转发信息，请执行步骤(4)。

```
<Sysname> display l2vpn forwarding pw verbose
VSI Name: aaa
  Link ID: 8
    PW Type          : VLAN                  PW State : Up
    In Label         : 1272                  Out Label: 1275
    MTU              : 1500
    PW Attributes    : Main
    VCCV CC          : Router-Alert
    VCCV BFD         : Fault Detection with BFD
    Flow Label       : Send
    Tunnel Group ID : 0x960000000
    Tunnel NHLFE IDs: 1034
    MAC limit        : maximum=2000   alarm=enabled   action=discard
```

(4) 执行 **display mpls lsp** 命令，查看是否存在承载 PW 的隧道，即是否存在 FEC 为 PW 对端 IP 地址的 LSP，若不存在，则需要先完成承载 PW 的隧道的建立。

```
<Sysname> display mpls lsp
FEC                       Proto    In/Out Label    Out Inter/NHLFE/LSINDEX
100.100.100.100/24        LDP      -/1049          GE1/0/1
```

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

- L2VPN/4/L2VPN_MACLIMIT_MAX_AC
- L2VPN/4/L2VPN_MACLIMIT_MAX_PW
- L2VPN/4/L2VPN_MACLIMIT_MAX_VSI

12 Segment Routing 故障处理

12.1 EVPN L3VPN over SRv6故障处理

12.1.1 EVPN L3VPN over SRv6 BE 流量转发不通

1. 故障描述

在 EVPN L3VPN over SRv6 组网中，采用 SRv6 BE 方式转发流量时，流量转发不通。

2. 常见原因

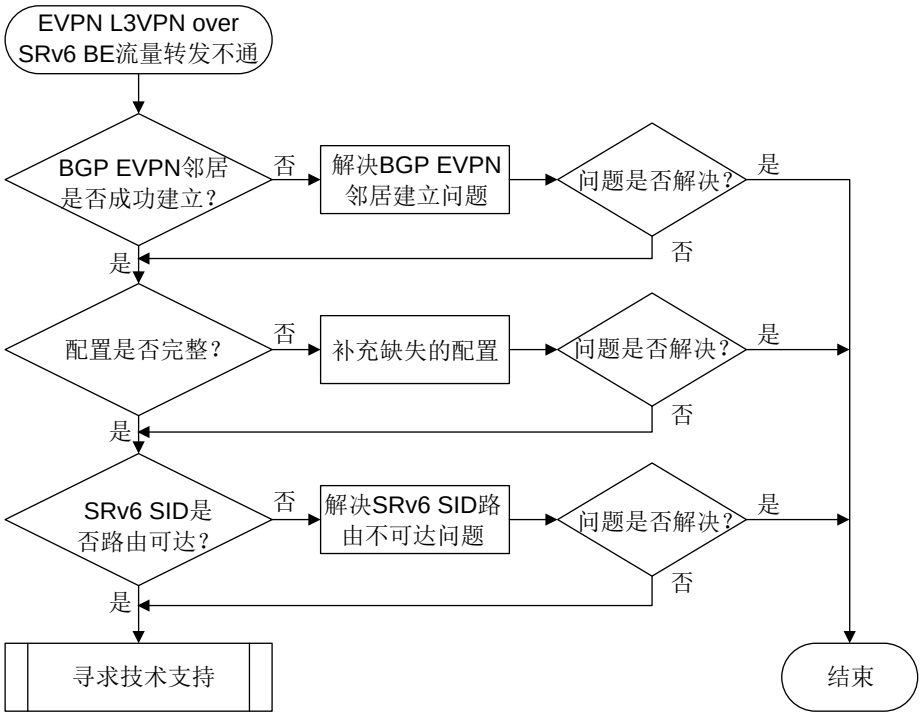
本类故障的常见原因主要包括：

- BGP EVPN 邻居未成功建立。
- EVPN L3VPN over SRv6 配置缺失。
- SRv6 SID 路由不可达。

3. 故障分析

本类故障的诊断流程如图 83 所示。

图83 EVPN L3VPN over SRv6 BE 流量转发不通的故障诊断流程图



4. 处理步骤

(1) 在本端 PE 设备上执行 **display bgp peer l2vpn evpn** 命令查看 BGP EVPN 邻居是否成功建立：

- 若显示信息中的 State 字段取值为 Established，则表示 PE 之间成功建立 BGP EVPN 邻居，请继续执行步骤(2)。

- 否则，请解决 BGP EVPN 邻居无法成功建立问题，解决方法请参见“BGP 邻居无法建立的定位思路”。

```
<Sysname> display bgp peer l2vpn evpn

BGP local router ID: 1.1.1.1
Local AS number: 100
Total number of peers: 1                 Peers in established state: 1

* - Dynamically created peer
Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State

2::2                   100       13       10    0        2 00:00:05 Established
```

(2) 检查两端 PE 设备上 EVPN L3VPN over SRv6 的配置是否完整。若不完整，请补充缺失的配置；若完整，请继续执行步骤(3)。

在两端 PE 上执行 **display current-configuration** 命令，检查是否存在以下配置。若不存在，则需要参见《EVPN L3VPN over SRv6 配置指导》手册，补充相关配置。

```
#
isis 1
 cost-style wide-compatible
 #
 address-family ipv6 unicast
  segment-routing ipv6 locator aaa        // 配置通过 IS-IS 通告 Locator 网段路由
#
#
bgp 100
 peer 3::3 as-number 100
 #
 address-family l2vpn evpn
  peer 3::3 enable
  peer 3::3 advertise encap-type srv6     // 配置向对等体/对等体组发布 SRv6 封装的 EVPN 路由
 #
 ip vpn-instance vpn1
  #
  address-family ipv4 unicast
   segment-routing ipv6 best-effort evpn  // 配置路由迭代到 SRv6 BE 隧道
   segment-routing ipv6 locator aaa evpn  // 配置 BGP 引用 Locator 段，以便在引用的 Locator 段内为指定 VPN 实例的私网路由申请 SRv6 SID
#
segment-routing ipv6
 encapsulation source-address 11::11      // 配置 SRv6 VPN 封装的 IPv6 报文头的源地址
 locator aaa ipv6-prefix 1:1:: 96 static 8  // 创建 Locator 段
#
```

(3) 在两端 PE 设备上分别检查是否存在到达对端的 SRv6 SID 的路由。

执行 **display ipv6 routing-table** *ipv6-address* 命令，查看是否存在到达 SRv6 SID 的路由。

```
<Sysname> display ipv6 routing-table 9::8000:2
```

```
Summary count : 1

Destination: 9::/64                                    Protocol  : IS_L1
NextHop    : FE80::8A1B:6FFF:FEDB:708                  Preference: 15
Interface  : GE1/0/3                                   Cost      : 20
```

若存在到达对端 SRv6 SID 的路由，则继续执行步骤(4)；否则，请解决无法通过 IGP 学习到路由的问题，解决方法请参见“IP 路由类故障处理手册”。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

12.1.2 EVPN L3VPN over SRv6 TE 流量转发不通

1. 故障描述

在 EVPN L3VPN over SRv6 组网中，采用 SRv6 TE 方式通过 SRv6 TE Policy 转发流量时，流量转发不通。

2. 常见原因

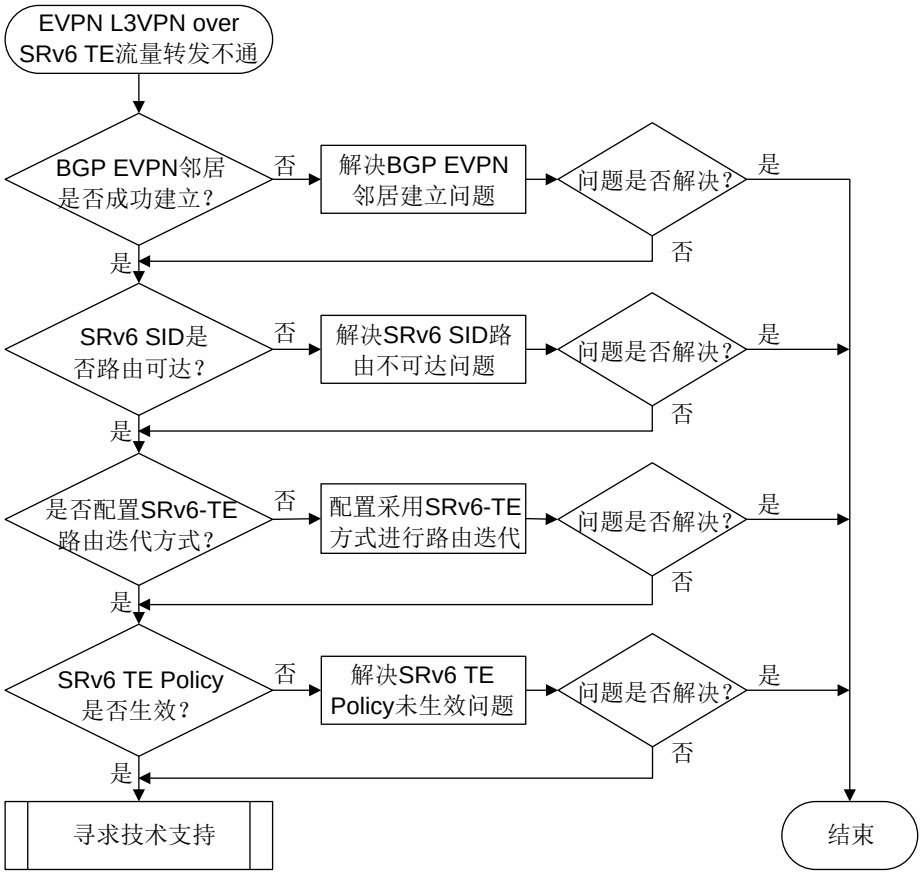
本类故障的常见原因主要包括：

- BGP EVPN 邻居未成功建立。
- SRv6 SID 路由不可达。
- BGP-VPN IPv4 单播地址族视图或 BGP-VPN IPv6 单播地址族视图下，未配置采用 SRv6 TE 方式进行路由迭代。
- EVPN 路由迭代到的 SRv6 TE Policy 没有生效。

3. 故障分析

本类故障的诊断流程如图 84 所示。

图84 EVPN L3VPN over SRv6 TE 流量转发不通的诊断流程图



4. 处理步骤

(1) 在本端 PE 设备上执行 **display bgp peer l2vpn evpn** 命令查看 BGP EVPN 邻居是否成功建立：

- 若显示信息中的 State 字段取值为 Established，则表示 PE 之间成功建立 BGP EVPN 邻居，请继续执行步骤(2)。
- 否则，请解决 BGP EVPN 邻居无法成功建立问题，解决方法请参见“BGP 邻居无法建立的定位思路”。

```
<Sysname> display bgp peer l2vpn evpn

 BGP local router ID: 1.1.1.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ  PrefRcv Up/Down  State
 2::2                   100       13       10    0        2 00:00:05 Established
```

(2) 在两端 PE 设备上分别检查是否存在到达对端的 SRv6 SID 的路由。

执行 **display ipv6 routing-table** *ipv6-address* 命令，查看是否存在到达 SRv6 SID 的路由。

```
<Sysname> display ipv6 routing-table 9::8000:2
```

```
Summary count : 1

Destination: 9::/64                                   Protocol  : IS_L1
NextHop    : FE80::8A1B:6FFF:FEDB:708                 Preference: 15
Interface  : GE1/0/3                                  Cost      : 20
```

若存在到达对端 SRv6 SID 的路由，则继续执行步骤(3)；否则，请解决无法通过 IGP 学习到路由的问题，解决方法请参见“IP 路由类故障处理手册”。

(3) 在BGP-VPN IPv4单播地址族视图或BGP-VPN IPv6单播地址族视图下，执行**display this**命令，查看当前配置中是否存在**segment-routing ipv6 traffic-engineering evpn**或者**segment-routing ipv6 traffic-engineering best-effort evpn**命令。若不存在上述命令，请补充配置该命令；否则，请继续执行步骤(4)。

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpn1
[Sysname-bgp-default-vpn1] address-family ipv4 unicast
[Sysname-bgp-default-ipv4-vpn1] display this
#
 segment-routing ipv6 locator aaa evpn
 segment-routing ipv6 traffic-engineering evpn
#
```

(4) 在两端 PE 设备上判断 EVPN 路由迭代到的 SRv6 TE Policy 是否有效。

在两端 PE 设备上执行**display segment-routing ipv6 te policy**命令，检查 SRv6 TE Policy 是否有效，即查看 Status 是否为 Down。若为 Down，则表示 SRv6 TE Policy 未生效，请参考“SRv6 TE Policy 无法生效的定位思路”解决该问题。

```
<Sysname> display segment-routing ipv6 te policy

Name/ID: p1/0
 Color: 10
 Endpoint: 1000::1
 Name from BGP:
 BSID:
  Mode: Dynamic              Type: Type 2              Request state: Succeeded
  Current BSID: 8000::1      Explicit BSID: -          Dynamic BSID: 8000::1
 Reference counts: 3
 Flags: A/BS/NC
 Status: Up
 AdminStatus: Up
 Up time: 2020-03-09 16:09:40
 Down time: 2020-03-09 16:09:13
…
```

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

12.2 SR-MPLS故障处理

12.2.1 SR-MPLS BE 方式的 SRLSP 无法建立

1. 故障描述

采用 SR-BE 方式建立 SRLSP 时，依次在 SRLSP 经过的各个节点上使用 **display mpls lsp** 命令检查 SRLSP 的标签交换信息，发现某个节点没有去往 SRLSP 的 Egress 节点的出标签（Out Label）或者该出标签并非 SR-MPLS 分配。例如，Egress 节点 FEC 为 5.5.5.5/32，如下显示表示该节点上不存在去往 5.5.5.5/32 的 SR-MPLS 出标签，即不存在去往 5.5.5.5/32 的 SRLSP。

```
<Sysname> display mpls lsp
FEC                       Proto       In/Out Label    Out Inter/NHLFE/LSINDEX
12.1.1.2                  Local       -/-             GE0/0/1
Tunnel1                   Local       -/-             NHLFE2
Tunnel10                  Local       -/-             NHLFE1
1.1.1.1/32                ISIS        16010/-         -
2.2.2.2/32                ISIS        16020/3         GE0/0/1
2.2.2.2/32                ISIS        -/3             GE0/0/1
3.3.3.3/32                ISIS        16030/16030     GE0/0/1
3.3.3.3/32                ISIS        -/16030         GE0/0/1
4.4.4.4/32                ISIS        16040/16040     GE0/0/1
4.4.4.4/32                ISIS        -/16040         GE0/0/1
1.1.1.1/1/4122            SR-TE       -/16030         GE0/0/1
                                      16040
```

2. 常见原因

本类故障的常见原因主要包括：

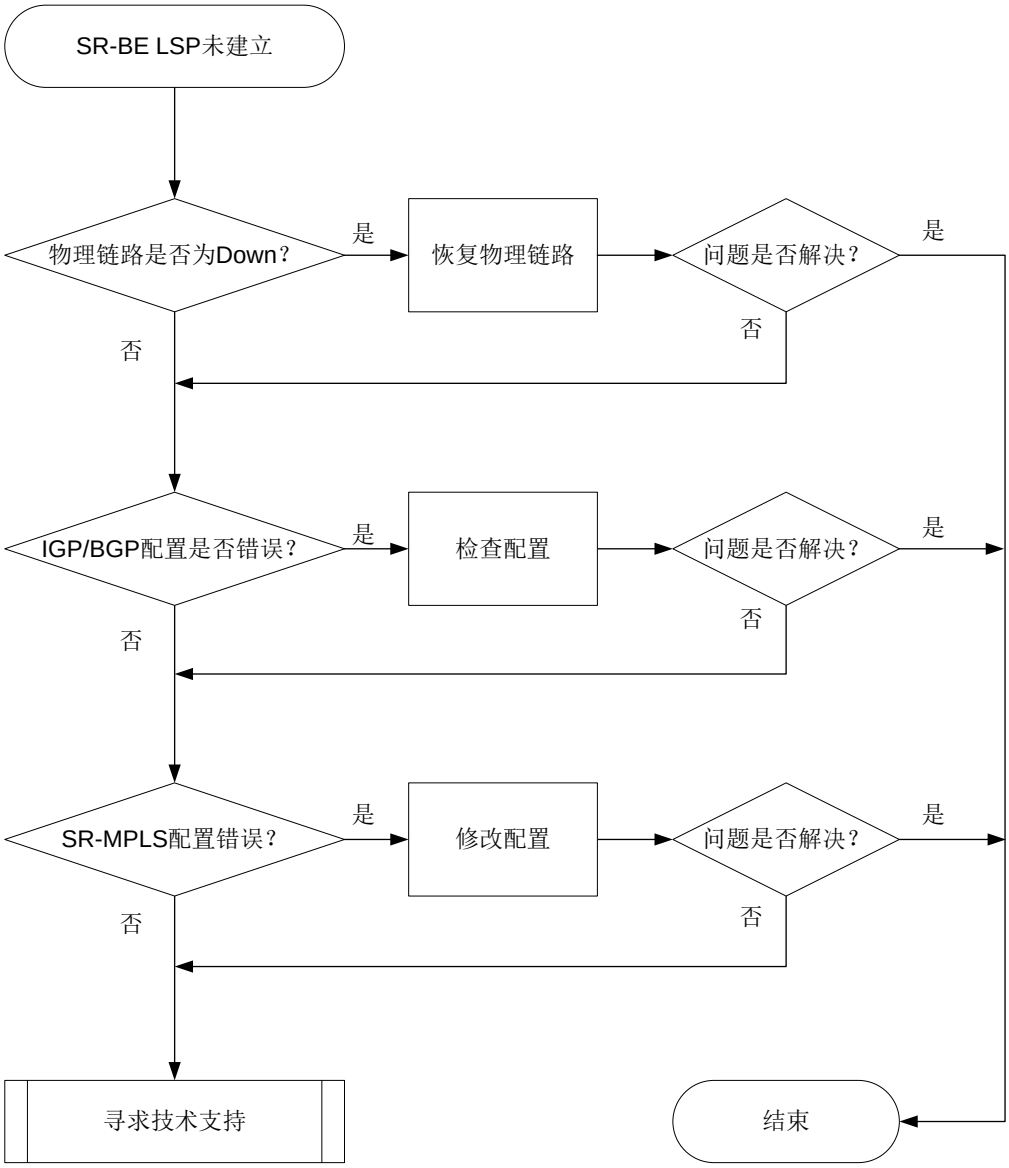
- 物理链路故障。
- IGP 或 BGP 邻居关系未正常建立导致 SR-MPLS 标签发布失败。
- SR-MPLS 配置缺少或错误。

采用 SR-BE 方式建立 SRLSP 完全依赖于 IGP 或 BGP 路由的发布，在 IGP 或 BGP 邻居之间通告路由信息时，需要携带 SR-MPLS 标签信息以建立 SRLSP。因此，IGP 或 BGP 邻居关系是否正常建立、IGP 路由是否正常发布是本类故障最重要的原因。

3. 故障分析

本类故障的诊断流程如图 85 所示。

图85 采用 SR-BE 方式无法建立 SRLSP 的故障诊断流程图



4. 处理步骤

(1) 在 SRLSP 经过的各个节点上通过命令 **display interface brief** 检查物理链路状态，确保 SRLSP 转发路径上各接口的物理状态和数据链路层协议状态均为 UP。如果链路正常，或链路恢复后问题仍未解决，请继续执行以下操作。

(2) 在 SRLSP 经过的各个节点上检查 IGP/BGP 邻居关系是否正常建立，IGP/BGP 配置是否正确。SR-MPLS 采用不同的路由协议发布标签时，故障处理方法有所不同：

- 如果使用 OSPF 作为 IGP 来通告路由信息并发布 SR-MPLS 标签：
  - 通过 **display ospf** 命令来判断 OSPF 是否使能 Opaque LSA 发布接收能力。如果 **display ospf** 命令显示信息中存在 Opaque capable 字段，表示 Opaque LSA 发布接收能力处于开启状态。若未使能该功能，则需要在 OSPF 视图下执行 **opaque-capability enable** 命令。

- 执行 **display ospf peer** 命令确认 OSPF 邻接关系是否正常。如果显示信息中邻居状态字段 State 显示为 Full，表示 OSPF 邻居关系正常。否则，请参见 OSPF 故障处理手册中“OSPF 邻居无法达到 FULL 状态”的处理过程。
- 执行 **display mpls lsp** 命令检查是否存在 OSPF 协议发布的 SR Prefix 方式的 LSP 信息。各节点的 SR Prefix SID 是管理员为 Loopback 地址手工指定的 SID。如果没有 SR Prefix 方式的 LSP 信息，请在各节点的 Loopback 接口视图下检查是否使用 **ospf area** 命令使能 OSPF 或在 OSPF 视图下是否使用 **network** 命令引入 Loopback 接口网段地址。

```
<Sysname> display mpls lsp
FEC                         Proto       In/Out Label    Out Inter/NHLFE/LSINDEX
1.1.1.9/32                  OSPF        16010/-         -
1.1.1.9/32                  ISIS        16010/-         -
2.2.2.9/32                  OSPF        16020/17020     RAGG1.4
```

- 如果**display mpls lsp**命令的显示信息中不仅存在OSPF协议发布的SRLSP信息，同时也存在 BGP 协议发布的相同 Prefix 的 SRLSP 信息，则可能因 Prefix SID 冲突导致 SRLSP 生成失败。此时请通过 **peer route-policy** 命令过滤掉从 BGP 对等体学习的该路由信息。

- 如果使用 IS-IS 作为 IGP 来通告路由信息并发布 SR-MPLS 标签：
  - 通过 **display isis** 命令的显示信息中 Cost style 字段来判断 IS-IS 开销值的类型是否为 wide、compatible 或 wide-compatible。如果 Cost style 字段的开销值类型不是以上三种，请执行 **cost-style** 命令来修改 IS-IS 开销值的类型。
  - 执行 **display isis peer** 命令确认 IS-IS 邻居关系是否正常。如果 **display isis peer** 命令邻居状态字段 State 显示为 Up，表示 IS-IS 邻居关系正常。否则，请参见 IS-IS 故障处理手册中“IS-IS 邻居无法建立”的处理过程。
  - 执行 **display mpls lsp** 命令检查是否存在 IS-IS 协议发布的 SR Prefix 方式的 LSP 信息。各节点的 SR Prefix SID 是管理员为 Loopback 地址手工指定的 SID。如果没有 SR Prefix 方式的 LSP 信息，请在各节点的 Loopback 接口视图下检查是否使用 **isis enable** 命令使能 IS-IS 功能。

```
<Sysname> display mpls lsp
FEC                         Proto       In/Out Label    Out Inter/NHLFE/LSINDEX
1.1.1.9/32                  OSPF        16010/-         -
1.1.1.9/32                  ISIS        16010/-         -
2.2.2.9/32                  ISIS        16020/17020     RAGG1.4
```

  - 如果 **display mpls lsp** 命令的显示信息中不仅存在 IS-IS 协议发布的 SRLSP 信息，同时也存在 BGP 协议发布的相同 Prefix 的 SRLSP 信息，则可能因 Prefix SID 冲突导致 SRLSP 生成失败。此时请通过 **peer route-policy** 命令过滤掉从 BGP 对等体学习的该路由信息。

- 如果使用 BGP 来通告路由信息并发布 SR-MPLS 标签：
  - 执行 **display bgp peer** 命令检查 BGP 对等体或对等体组的邻居关系是否正常。如果 **display bgp peer** 命令 BGP 会话的状态字段 State 显示为 Established，表示 BGP 对等体或对等体组邻居关系正常。否则，请参见 BGP 故障处理手册中“BGP 邻居无法建立”的处理过程。

– 执行 **display mpls lsp** 命令检查是否存在 BGP 协议发布的 SR Prefix 方式的 LSP 信息。如果没有，请检查 BGP 的指定对等体/对等体组配置了 **peer label-route-capability** 命令来使能交换带标签路由的能力，并且通过路由策略为引入 BGP 的 Loopback 地址配置了标签索引值。

```
<Sysname> display mpls lsp
FEC                         Proto       In/Out Label    Out Inter/NHLFE/LSINDEX
1.1.1.9/32                  OSPF        16010/-         -
1.1.1.9/32                  ISIS        16010/-         -
2.2.2.9/32                  BGP         16020/17020     RAGG1.4
```

如果执行以上操作后，问题仍未解决，则请继续执行以下操作。

(3) 在 SRLSP 经过的各个节点上检查 SR-MPLS 配置。

a. 在 IS-IS 视图、OSPF 视图或 BGP 视图下检查是否开启支持 SR-MPLS 功能。如果未开启支持 SR-MPLS 功能，则在 IS-IS 视图、OSPF 视图或 BGP 视图下执行 **segment-routing mpls** 命令开启该功能。

b. SR-BE LSP 使用前缀 SID 方式建立 SRLSP 转发路径，请在 LoopBack 接口视图下检查是否配置前缀 SID。如果未配置，则在 OSPF 视图下执行 **ospf prefix-sid** 命令或在 IS-IS 视图下执行 **isis prefix-sid** 命令配置前缀 SID。

c. 执行 **display segment-routing label-block** 命令检查 LoopBack 接口下配置的前缀 SID 是否在 SRGB 标签段范围内。如果前缀 SID 未在 SRGB 范围内，则请修改配置的前缀 SID，否则该 SID 不会生效。

d. 如果执行以上操作后，问题仍未解决，则请继续执行以下操作。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

12.2.2 SR-MPLS TE Tunnel 状态为 Down

1. 故障描述

在 Ingress 上执行 **display mpls te tunnel-interface** 命令检查 SR-MPLS TE Tunnel 的状态为 Down。

```
<Sysname> display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel Signalled Name  : tunnel1
Tunnel State           : Down (Main CRLSP Down. Backup CRLSP Down.)
...
```

2. 常见原因

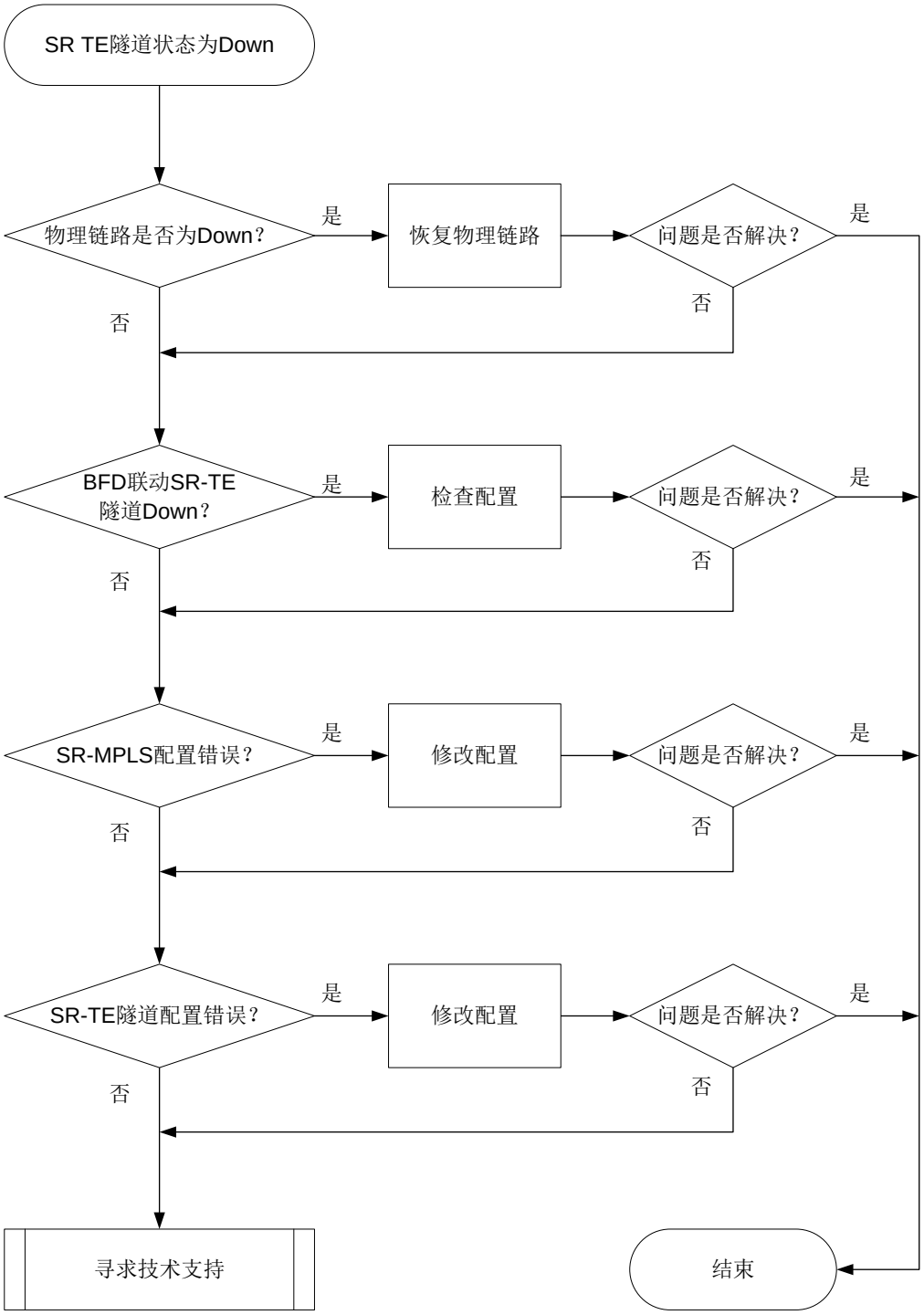
本类故障的常见原因主要包括：

- 构成 SR-MPLS TE Tunnel 的 SRLSP 所经过的路径上存在物理链路故障。
- 用于检测 SR-MPLS TE Tunnel 的 BFD 会话状态为 down，使得 SR-MPLS TE Tunnel 状态为 Down。
- SR-MPLS 配置缺少或错误。
- SR TE Tunnel 配置错误。

3. 故障分析

本类故障的诊断流程如图 86 所示。

图86 SR-MPLS TE Tunnel Down 的故障诊断流程图



4. 处理步骤

(1) 在 SRLSP 经过的各个节点上通过命令 **display interface brief** 检查物理链路状态，确保 SRLSP 转发路径上各接口的物理状态和数据链路层协议状态均为 UP。如果链路正常，或链路恢复后问题仍未解决，请继续执行以下操作。

(2) 检查是否由 BFD 会话 Down 导致 SR TE Tunnel Down。

a. 在 SR-MPLS TE 隧道接口下使用 **display this** 命令检查是否配置了 **mpls bfd** 命令。如果配置了，则执行 b。

b. 使用 **display mpls bfd** 命令检查 BFD/SBFD 会话的状态。如果 BFD/SBFD 会话的状态为 Down，则执行 c。

c. 可能是由于BFD联动导致SR-TE隧道Down，请执行**undo mpls bfd**命令删除BFD/SBFD检测相关命令。如果 BFD/SBFD 会话正常或者不存在 BFD/SBFD 会话，问题仍未解决请执行(3)。

(3) 检查 SR-MPLS 配置。

a. 在 IS-IS 视图或 OSPF 视图下检查是否开启支持 SR-MPLS 功能，同时需要检查以下配置，否则 SR-MPLS 功能不会生效：

- 当 IGP 协议为 IS-IS 时，通过 **display isis** 命令的显示信息中 Cost style 字段来判断 IS-IS 开销值的类型是否为 wide、compatible 或 wide-compatible。如果 Cost style 字段的开销值类型不是以上三种，请执行 **cost-style** 命令来修改 IS-IS 开销值的类型。
- 当IGP协议为OSPF时，通过**display ospf**命令来判断OSPF是否使能Opaque LSA发布接收能力。如果 **display ospf** 命令显示信息中存在 Opaque capable 字段，表示 Opaque LSA 发布接收能力处于开启状态。若未使能该功能，则需要在 OSPF 视图下执行 **opaque-capability enable** 命令。

b. 若使用前缀 SID 方式建立 SRLSP 转发路径，请在 LoopBack 接口视图下检查是否配置了前缀 SID。如果未配置，则在 OSPF 视图下执行 **ospf prefix-sid** 命令或在 IS-IS 视图下执行 **isis prefix-sid** 命令配置前缀 SID；若使用 Adjacency SID 方式建立 SRLSP 转发路径，请在 OSPF 视图或 IS-IS 视图下开启邻接标签分配功能或者在 SRLSP 转发路径的接口上检查是否配置了 Adjacency SID。如果未配置，则在 OSPF 视图或 IS-IS 视图下执行 **segment-routing adjacency enable** 命令开启邻接标签分配功能。也可以在接口视图下执行 **isis adjacency-sid** 命令或 **ospf adjacency-sid** 命令配置 Adjacency SID。

c. 执行 **display segment-routing label-block** 命令检查 LoopBack 接口下配置的前缀 SID 是否在 SRGB 标签段范围内，并检查接口下配置的 Adjacency SID 是否在 SRLB 标签段范围内。如果前缀 SID 未在 SRGB 范围内或者 Adjacency SID 未在 SRLB 标签段范围内，则请修改配置的 Adjacency SID，否则该 SID 不会生效。

d. 如果执行以上操作后，问题仍未解决，则请继续执行以下操作。

(4) 检查 TE 隧道配置。MPLS TE 采用不同方式生成 SRLSP 时，故障定位方式有所不同：

- MPLS TE 隧道采用静态指定标签生成 SRLSP：在 SRLSP 的 Ingress 上执行 **display mpls static-sr-mpls** 命令查看静态 SRLSP 信息或静态配置的邻接段信息，保证出标签栈字段Out-Label表示的标签序列依次和SRLSP路径上各节点配置的静态标签值一一对应。如果 Ingress 上出标签栈中的标签序列与 SRLSP 路径上各节点配置的静态标签值不对应，请执行 **static-sr-mpls lsp** 命令修改 Ingress 上出标签栈中的标签序列。
- 若 MPLS TE 隧道采用显式路径算路生成 SRLSP：在 SRLSP 的 Ingress 上执行 **display explicit-path** 命令检查显式路径上节点的 IP 地址或者 SID 与 SRLSP 路径上各节点的 IP 地址或者本地 SID 一一对应，并保证 Ingress 上显式路径视图下通过 **nexthop** 命令指定的 SID 类型与 SRLSP 路径上各节点的接口视图下配置的前缀 SID 或 Adjacency SID 类型保持一致，即接口下配置了前缀 SID，**nexthop** 命令指定的 SID 也必须是前缀 SID。如果存在问题，请通过 **nexthop** 命令修改显式路径上的 IP 地址或者 SID。

- 若 MPLS TE 隧道采用 PCE 托管方式由控制器算路生成 SRLSP，请检查 SR-TE Tunnel 接口下是否执行了 **mpls te delegation** 命令开启了 SRLSP 托管功能，并执行命令 **display mpls te pce peer** 检查 PCC 与 PCE 是否建立了 PCEP 会话。通过抓包确认控制器（PCE）是否进行了路径更新以及路径是否正确。在抓取报文中请确保由 PCE 下发的 Adjacency SID 或下一跳地址使用 strict 方式，前缀 SID 或者节点地址使用 loose 方式。如果 PCC 与 PCE 未正常建立了 PCEP 会话，且抓取报文未满足上述要求，请检查控制器上的配置。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- TE/5/TE_BACKUP_SWITCH

12.3 SRv6 TE Policy故障处理

12.3.1 SRv6 TE Policy 无法生效的定位思路

1. 故障描述

执行 **ping srv6-te policy** 命令检查指定 SRv6 TE Policy 的连通性时，发现报文无法通过 SRv6 TE Policy 正常转发。例如：

```
<Sysname> ping srv6-te policy policy-name p1
The SRv6-TE policy does not reference a SID list or the referenced SID list is down.
```

2. 常见原因

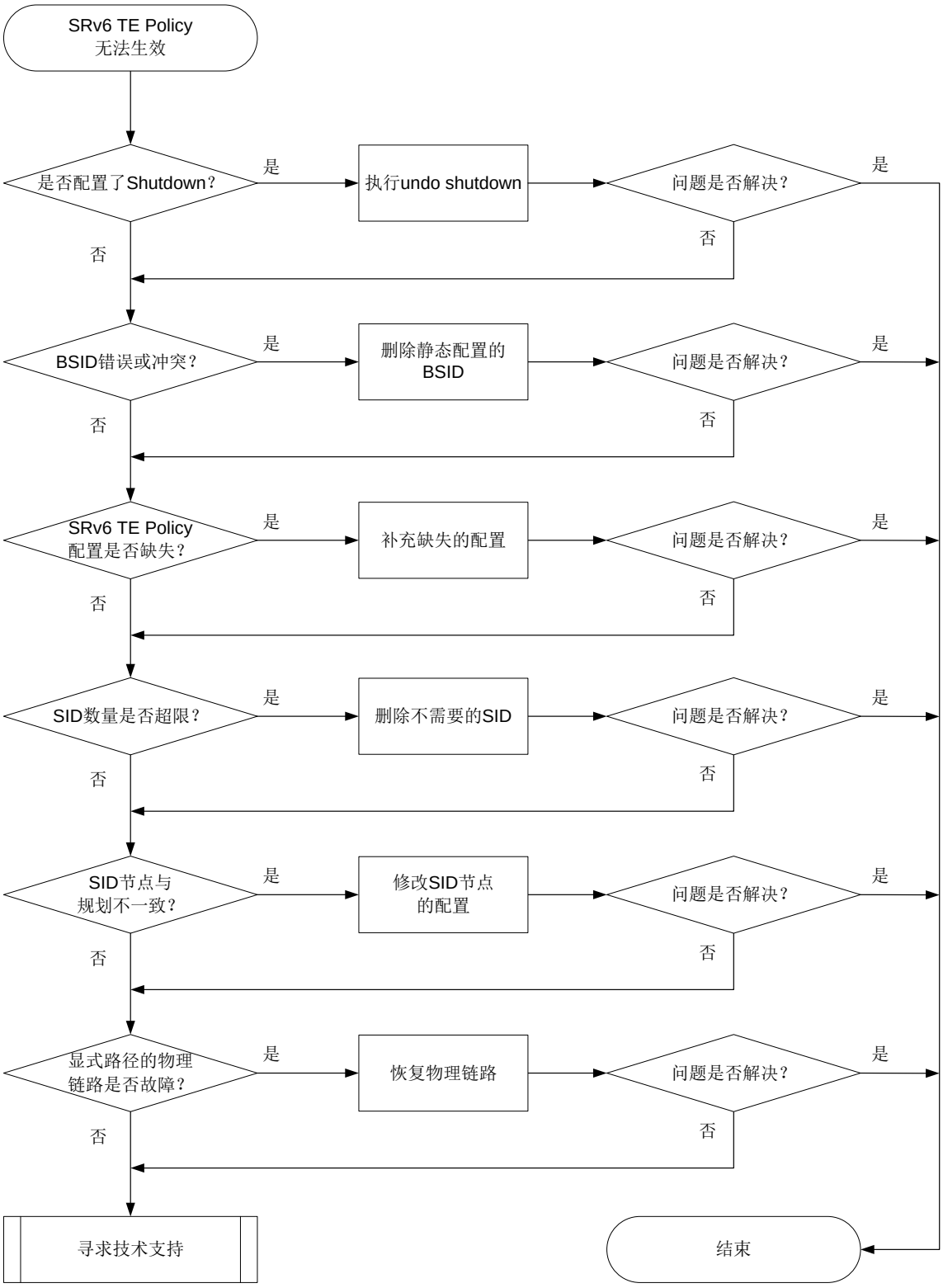
本类故障的常见原因主要包括：

- SRv6 TE Policy 状态为 Shutdown。
- SRv6 TE Policy 的 BSID 配置错误或者冲突。
- SRv6 TE Policy 下配置缺失。
- Segment List 中 SID 数量超限。
- SRv6 TE Policy 的 SID 列表与报文转发路径的规划不同。
- SRv6 TE Policy 报文转发路径上的物理链路故障。

3. 故障诊断流程

本类故障的诊断流程如图 87 所示。

图87 SRv6 TE Policy 无法生效的故障诊断流程图



4. 故障处理步骤

(1) 在 SRv6 TE Policy 的头节点执行 **display segment-routing ipv6 te policy status** 命令初步查看 SRv6 TE Policy 不生效的原因。

```
<Sysname> display segment-routing ipv6 te policy status
Name/ID: p1/0
Status: Down
  Check admin status                  : Failed
  Check for endpoint & color          : Passed
  Check for segment list              : Passed
  Check valid candidate paths         : Failed
  Check for BSIDs                     : -
```

如果 Check admin status 字段显示为 Failed，说明 SRv6 TE Policy 处于管理关闭状态。请进入指定 SRv6 TE Policy 视图下执行 **undo shutdown** 命令，设置 SRv6 TE Policy 为开启状态。

开启指定 SRv6 TE Policy 后，再次执行 **display segment-routing ipv6 te policy status** 命令，如果存在其他校验字段显示为 Failed 或“-”，例如 Check for segment List 字段显示为 Failed，请继续执行以下操作。

(2) 检查 SRv6 TE Policy 的 BSID 是否存在冲突。

在 SRv6 TE Policy 的头节点执行 **display segment-routing ipv6 te policy** 命令。显示信息中 Request state 字段取值为 Failed 表示 BSID 申请失败。请确认静态指定的 BSID 可能不在 **srv6-policy locator** 命令用来引用的 Locator 段范围内或者与已存在的 SRv6 TE Policy 的 BSID 出现重复，从而导致 SRv6 TE Policy 失效。建议在失效的 SRv6 TE Policy 下执行 **undo binding-sid** 命令删除静态手工指定 BSID，由系统自动申请 BSID，以避免错误和冲突。

```
<Sysname> display segment-routing ipv6 te policy

Name/ID: p1/0
 Color: 10
 Endpoint: 1000::1
 Name from BGP:
 BSID:
  Mode: Dynamic              Type: Type 2              Request state: Succeeded
  Current BSID: 8000::1      Explicit BSID: -          Dynamic BSID: 8000::1
 Reference counts: 3
 Flags: A/BS/NC
```

如果 BSID 申请成功以后，问题仍未解决，则请继续执行以下操作。

(3) 检查 SRv6 TE Policy 的配置是否完整。

以 IS-IS 作为 IGP 通告 SID 为例，在 SRv6 TE Policy 的头节点上执行命令 **display current-configuration**，查看配置是否与以下实例中的一致。如果缺少任意一项，则说明遗漏了部分配置。

```
isis 1
address-family ipv6 unicast
  segment-routing ipv6 locator a

segment-routing ipv6
```

```
locator a ipv6-prefix 1000:0:0:1:: 64 static 16
traffic-engineering
  srv6-policy locator a
  segment-list sl1
   index 10 ipv6 1000::2:0:0:1:0
   index 20 ipv6 1000::2:0:0:1:3
  policy p1
   color 100 end-point ipv6 4::4
   candidate-paths
    preference 100
     explicit segment-list sl1
```

SRv6 TE Policy 报文转发路径的各节点上，也需要在 IGP 视图下配置 **segment-routing ipv6 locator** 命令，以正常发布 Locator 段。例如：

```
isis 1
address-family ipv6 unicast
  segment-routing ipv6 locator b
```

如果配置不完整，请补充缺失配置。配置补充完整后，如果问题仍未解决，请继续执行以下操作。

(4) 检查 Segment List 中 SID 数量是否超限。

在 SRv6 TE Policy 头节点上进入 probe 视图，并执行 **display system internal segment-routing ipv6 te policy status** 命令，显示信息中 MaxSIDs 表示 Segment List 中 SID 的数量上限。

```
[Sysname-probe] display system internal segment-routing ipv6 te policy status
…
   MaxGroupNidNum: 1024           MaxPolicyNidNum: 1024
 MaxSeglistNidNum: 4096         MaxNexthopNidNum: 65535
        MaxOutNum: 32                 MaxEcmpNum: 128
          MaxSIDs: 10
…
```

执行 **display segment-routing ipv6 te segment-list** 命令，显示信息中的 Nodes 字段表示该指定 Segment List 中配置的 SID 节点数量。

```
<Sysname> display segment-routing ipv6 te segment-list

Total Segment lists: 1

Name/ID: A/1
 Origin: CLI
 Status: Up
 Nodes: 11
…
```

如果配置的 SID 节点数量超过 SID 的数量上限，请删除 Segment List 中不必要的 SID 值。如果配置的 SID 节点数量未超过上限，请继续执行以下操作。

(5) 检查 SID 列表的配置与规划是否一致。

在 SRv6 TE Policy 头节点执行 **display segment-routing ipv6 te segment-list** 命令，显示 SID 列表信息，其中自上而下依次排列的 SID 值表示转发路径上距离 SRv6 TE

Policy 头节点由近到远的各节点或链路。请使用 **display ipv6 routing-table** 检查 SID 列表中所有 SID 值均通过路由协议正常学习到，如果未正常学习到，请检查 OSPFv3 或 IS-IS 配置，参考 OSPFv3 或 IS-IS 故障处理手册检查路由学习问题。

```
[Sysname] display segment-routing ipv6 te segment-list

Total Segment lists: 1

Name/ID: s1/1
 Origin: CLI
 Status: Down
 Nodes : 3

  Index    : 10                              SID: 1::1
  Type     : Type_2                        Flags: None

  Index    : 20                              SID: 1::2
  Type     : Type_2                        Flags: None

  Index    : 30                              SID: 1::3
  Type     : Type_2                        Flags: None
```

在 SRv6 TE Policy 转发路径上的各个节点上依次执行 **display segment-routing ipv6 local-sid** 命令查看 SID 值是否与上述命令显示的 SID 列表中的 SID 值一致。SID 类型通常为 End SID 或 End.X SID。例如，对于 End SID，查看 SRv6 Local SID 的信息。

```
[Sysname] display segment-routing  ipv6  local-sid end
                    Local SID forwarding table (End)
Total SIDs: 2

SID           : 1000::2:0:0:1:0/64
Function type : End                             Flavor         : PSP
Locator name  : b                               Allocation type: Dynamic
Owner         : IS-IS-1                         State          : Active
Create Time   : Sep 04 16:32:03.443 2021
```

如果 SID 列表与转发路径上各节点的 SID 值不一致，请执行 **undo index** *index-number* 命令删除错误的 SID，再执行 **index** *index-number* **ipv6** *ipv6-address* 命令重新配置正确的 SID。如果 SID 列表与规划一致，请继续执行以下操作。

(6) 在 SRv6 TE Policy 转发路径上的各个节点上通过 **display interface brief** 命令检查物理链路状态，确保转发路径上各接口的物理状态和数据链路层协议状态均为 UP。如果链路正常，或链路恢复后问题仍未解决，请继续执行以下操作。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- SRPV6/2/SRPV6_BSID_CONFLICT
- SRPV6/2/SRPV6_BSID_CONFLICT_CLEAR
- SRPV6/5/SRPV6_PATH_STATE_DOWN
- SRPV6/4/SRPV6_POLICY_STATUS_CHG
- SRPV6/4/SRPV6_RESOURCE_EXDCEED
- SRPV6/4/SRPV6_RESOURCE_EXCEED_CLEAR
- SRPV6/5/SRPV6_SEGLIST_STATE_DOWN
- SRPV6/5/SRPV6_ SEGLIST_STATE_DOWN
- SRPV6/2/SRPV6_STATE_DOWN
- SRPV6/2/SRPV6_STATE_DOWN_CLEAR

13 VXLAN 类故障处理

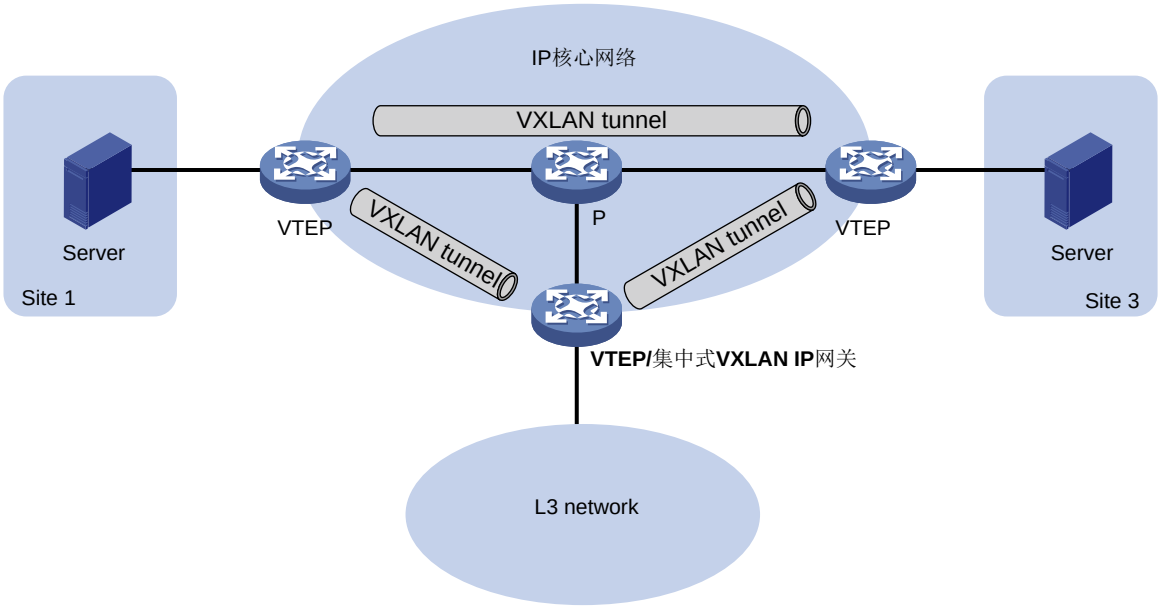
13.1 VXLAN故障处理

13.1.1 Ping 不通集中式 VXLAN IP 网关

1. 故障描述

如图 88 所示，VTEP 与集中式 VXLAN IP 网关之间建立 VXLAN 隧道，集中式 VXLAN IP 网关上 VSI 虚接口作为网关接口。配置完成后，在 VTEP 连接的服务器上执行 Ping 操作，发现 Ping 不通集中式 VXLAN IP 网关。

图88 集中式 VXLAN IP 网关示意图



2. 常见原因

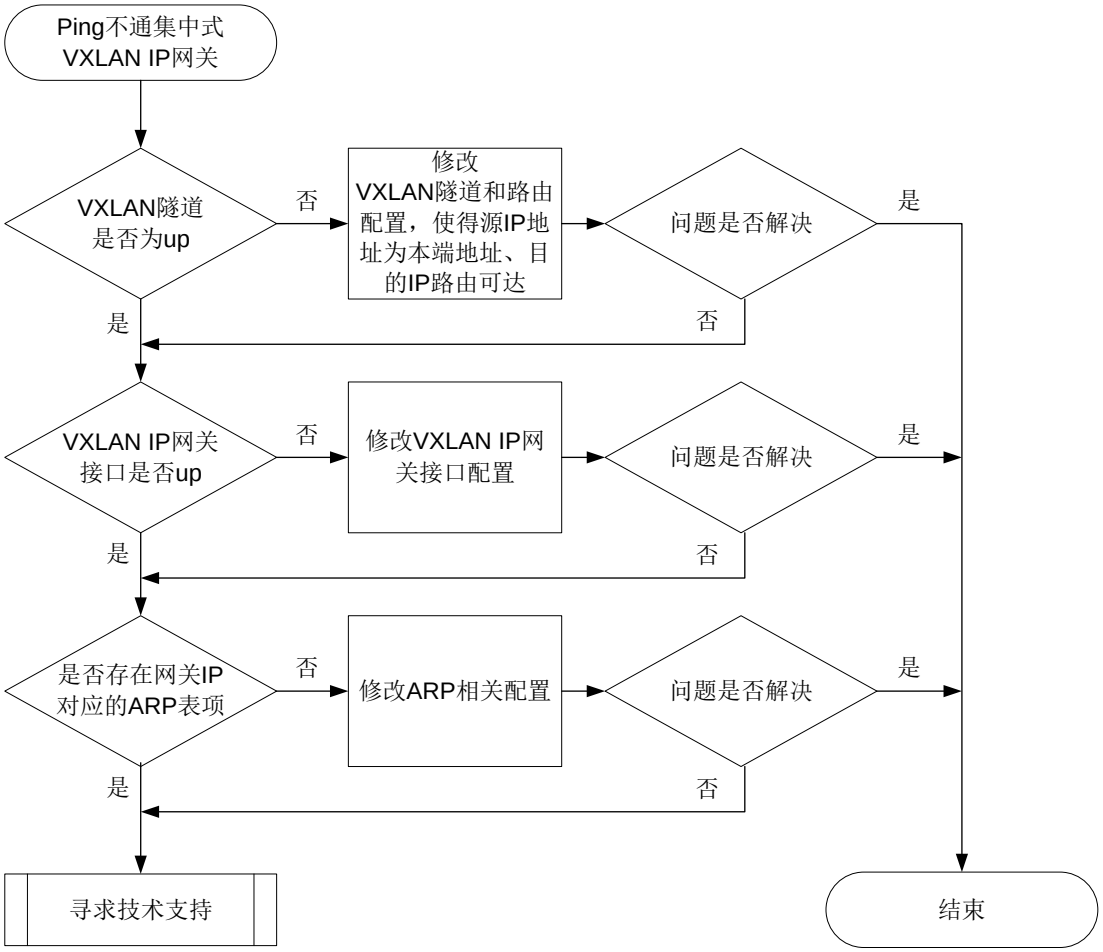
本类故障的常见原因主要包括：

- VXLAN 隧道状态为 Down。
- VXLAN 隧道的源 IP 或目的 IP 配置错误。
- VXLAN IP 网关接口状态为 Down。
- 设备上不存在 ping 命令对应的 ARP 表项。

3. 故障分析

本类故障的诊断流程如图 89 所示。

图89 Ping 不通集中式 VXLAN IP 网关的故障诊断流程图



4. 处理步骤

(1) 在连接服务器的 VTEP 上查看服务器所属的 VXLAN 网络的 VXLAN 隧道信息。

a. 执行 **display l2vpn vsi verbose** 命令查看服务器所属的 VXLAN 网络的 VXLAN ID 以及与 VXLAN 网络关联的 VXLAN 隧道的名称（Tunnel Name 字段）。

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
...
  VXLAN ID                : 10
```

```
Tunnels:
  Tunnel Name          Link ID    State  Type        Flood proxy
  Tunnel1              0x5000001  Up     Manual      Disabled
  Tunnel2              0x5000002  Up     Manual      Disabled
ACs:
   AC                              Link ID    State    Type
   GE1/0/1 srv1000                 0          Up       Manual
```

b. 根据 VXLAN 隧道的名称执行 **display interface tunnel** 命令，查看服务器接入的 VXLAN 网络内 VXLAN 隧道的状态（Current state）、隧道的源 IP 地址（Tunnel source）和隧道的目的 IP 地址（destination）。

```
<Sysname> display interface tunnel 2
Tunnel2
Current state: UP
Line protocol state: UP
Description: Tunnel2 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 2.2.2.2, destination 1.1.1.1
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

– 若 VXLAN 隧道为 Up 状态，请继续执行第(3)步。

– 若 VXLAN 隧道为 Down 状态，请继续执行第(2)步。

(2) 在 VTEP 上查看 VXLAN 隧道的源 IP 地址是否为本端的 IP 地址、目的 IP 地址是否可达。

- 执行 **display ip interface brief** 命令，查看 VXLAN 隧道的源 IP 地址是否为本端的 IP 地址。若 VXLAN 隧道的源 IP 地址不是本端的 IP 地址，请通过 **source** 命令修改 VXLAN 隧道的源 IP 地址。

```
<Sysname> display ip interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface           Physical Protocol IP address      VPN instance Description
Loop1               up       up(s)    2.2.2.2         --           --
...
```

- 执行 **display fib** 命令，查看 FIB 表中是否存在到达 VXLAN 隧道的目的 IP 地址的表项。若不存在对应的表项，请修改路由配置，确保 VXLAN 隧道的目的 IP 地址路由可达。

```
<Sysname> display fib
...
Destination/Mask    Nexthop         Flag     OutInterface/Token       Label
0.0.0.0/32          127.0.0.1       UH       InLoop0                  Null
2.2.2.2/32          127.0.0.1       UH       InLoop0                  Null
1.1.1.1/32          127.0.0.1       UH       InLoop0                  Null
```

```
127.0.0.0/32       127.0.0.1       UH       InLoop0                  Null
```

(3) 在 VXLAN IP 网关上执行 **display interface vsi-interface brief** 命令，查看 VXLAN IP 网关接口信息，包括网关接口编号（Interface）、网关接口状态（Link Protocol）和网关 IP 地址（Primary IP）。

```
<Sysname> display interface Vsi-interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Vsi1                 DOWN DOWN     192.168.1.1
```

- 若 VXLAN IP 网关接口为 Down 状态，请查看 VSI 虚接口下是否配置了 **shutdown** 命令或绑定 VSI 虚接口的 VSI 是否为 Up 状态。
  - 若 VSI 虚接口下配置了 **shutdown** 命令，请执行 **undo shutdown** 命令。
  - 若绑定 VSI 虚接口的 VSI 为 Down 状态，请执行 **display l2vpn vsi** 命令，查看 VSI 下 AC 的状态。若 AC 的状态为 Down，则检查 AC 配置是否正确和 AC 所在的接口是否 Up。如果 AC 配置不正确或 AC 所在的接口为 Down 状态，请修改 AC 配置或排查接口故障。
- 若 VXLAN IP 网关接口为 Up 状态，请执行 **display arp** 命令查看是否学习到了网关 IP 对应的 ARP 信息。

```
<Sysname> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address       MAC address    VLAN/VSI  Interface/Link ID        Aging Type
10.1.1.1         0001-0001-0001 0         Tunnel2                  17    D
10.1.1.11        0001-0001-0001 0         Tunnel2                  20    D
20.1.1.1         0002-0002-0002 1         Tunnel3                  17    D
20.1.1.12        0002-0002-0002 1         Tunnel3                  20    D
```

  - 若存在网关 IP 对应的 ARP 信息，请继续执行第(4)步。
  - 若不存在网关 IP 对应的 ARP 信息，请执行 **display arp count** 命令查看学习的表项数目是否达到了设备/接口配置的动态 ARP 表项的最大数目。如果达到动态 ARP 表项的最大数目，请执行 **arp max-learning-num/arp max-learning-number** 命令将允许学习的动态 ARP 表项的最大数目调大。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无

相关日志

无

14 EVPN 类故障处理

14.1 EVPN VXLAN故障处理

14.1.1 EVPN 分布式网关场景，同一 VXLAN 内的 VTEP 之间隧道无法建立

1. 故障描述

EVPN 分布式网关场景，同一 VXLAN 内的 VTEP 之间隧道无法建立。

2. 常见原因

本类故障的常见原因主要包括：

- 未收到 EVPN 的 2 类路由（MAC/IP 发布路由）、3 类路由（IMET 路由）。
- EVPN 实例下的 RT 配置错误。

3. 故障分析

本类故障的诊断思路如下：

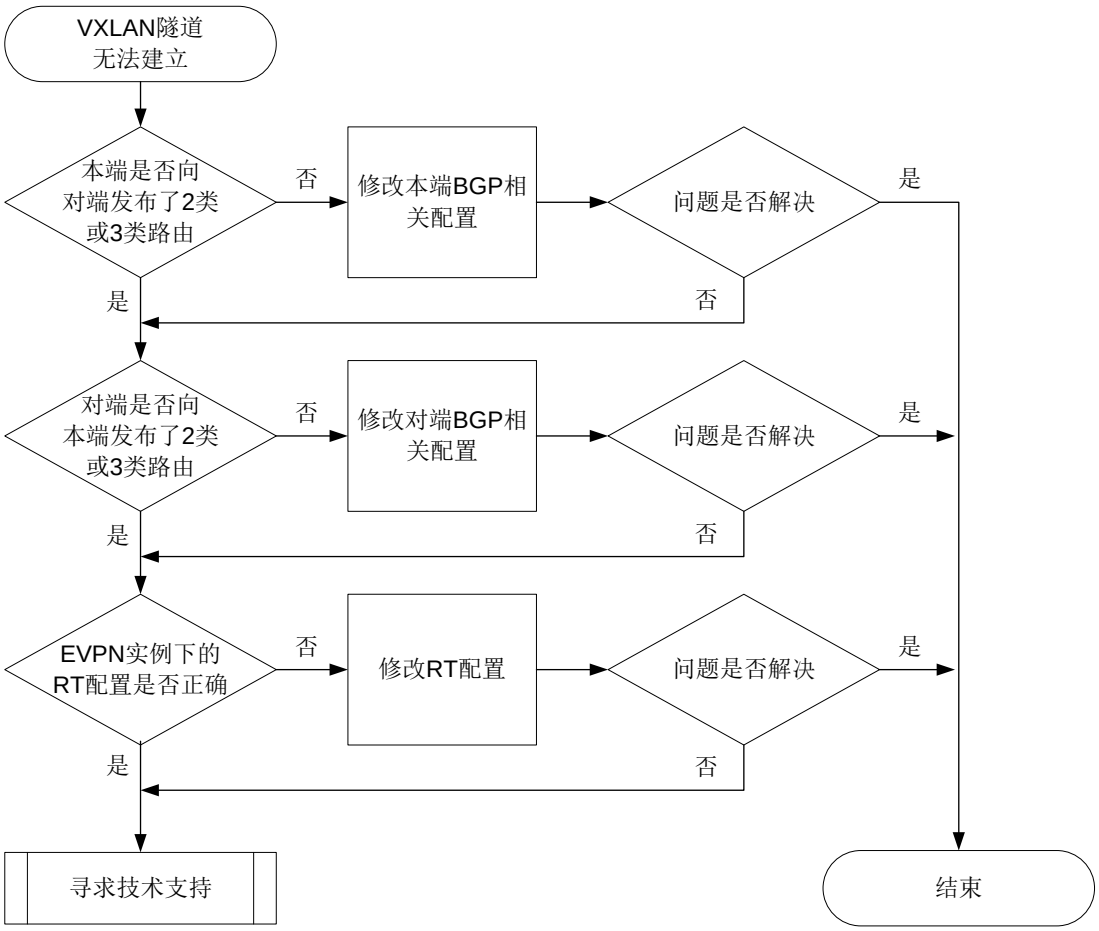
(1) 检查是否收到 2 类路由。

(2) 检查是否收到 3 类路由。

(3) 检查 EVPN 实例下的 RT 是否配置错误。

同一 VXLAN 内 VTEP 之间的 VXLAN 隧道无法建立的故障诊断流程如图 90 所示。

图90 同一 VXLAN 内 VTEP 之间的 VXLAN 隧道无法建立的故障诊断流程图



4. 处理步骤

同一 VXLAN 内 VTEP 之间的 VXLAN 隧道无法建立时，故障处理步骤如下：

(1) 在本端执行 **display bgp l2vpn evpn** 命令查看本端是否向对端发布了 2 类或 3 类路由。例如，下面的显示信息表示本端向 4.4.4.4 通告了 2 类和 3 类路由。如果组网中存在 RR，则 **display bgp l2vpn evpn** 命令需要指定 RR 的地址；否则，需要指定对端的地址。

```
<Sysname> display bgp l2vpn evpn peer 4.4.4.4 advertised-routes

 Total number of routes: 2

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external,
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 2:2
 Total number of routes: 2

     Network            NextHop         MED        LocPrf             Path/Ogn
```

```
* >  [2][0][48][0e86-19b6-0308][0][0.0.0.0]/104
                        0.0.0.0         0          100                i
* >  [3][0][32][1.1.1.1]/80
                        0.0.0.0         0          100                i
```

- 如果本端向对端发布了 2 类或 3 类路由，则执行第(2)步。
- 如果本端未向对端发布 2 类和 3 类路由，请检查 EVPN 功能中 BGP 的相关配置是否正确，具体配置参见“EVPN 配置指导”中的“EVPN VXLAN”。

(2) 在对端执行 **display bgp l2vpn evpn** 命令查看对端是否向本端发布了 2 类或 3 类路由。例如，下面的显示信息表示对端向 4.4.4.4 通告了 2 类和 3 类路由。如果组网中存在 RR，则 **display bgp l2vpn evpn** 命令需要指定 RR 的地址；否则，需要指定对端的地址。

```
<Sysname> display bgp l2vpn evpn peer 4.4.4.4 advertised-routes

 Total number of routes: 2

 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external,
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 1:1
 Total number of routes: 2

     Network            NextHop         MED        LocPrf             Path/Ogn

* >  [2][0][48][0e86-23cf-0507][0][0.0.0.0]/104
                        0.0.0.0         0          100                i
* >  [3][0][32][3.3.3.3]/80
                        0.0.0.0         0          100                i
```

- 如果对端向本端发布了 2 类或 3 类路由，则执行第(3)步。
- 如果对端未向本端发布 2 类和 3 类路由，请检查 EVPN 功能中 BGP 的相关配置是否正确，具体配置参见“EVPN 配置指导”中的“EVPN VXLAN”。

(3) 在 VSI 视图下执行 **display this** 命令查看两端的 Export target 属性与 Import target 属性配置是否正确。

```
[Sysname-vsi-aaa] display this
#
vsi aaa
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher 2:2
  vpn-target 1:1 export-extcommunity
  vpn-target 2:2 import-extcommunity
#
return
```

- 如果两端的 RT 属性不匹配，请在 VSI 视图下执行 **vpn-target** 命令修改 Route Target 属性配置。
- 如果两端的 RT 属性匹配，则执行第(4)步。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

无。

14.1.2 EVPN 分布式网关场景，不同 VXLAN 内的 VTEP 之间隧道无法建立

1. 故障描述

EVPN 分布式网关场景，不同 VXLAN 内的 VTEP 之间隧道无法建立。

2. 常见原因

本类故障的常见原因主要包括：

- 未收到 EVPN 的 2 类路由、5 类路由（IP 前缀路由）。
- VPN 实例下的 RT 配置错误。

3. 故障分析

本类故障的诊断思路如下：

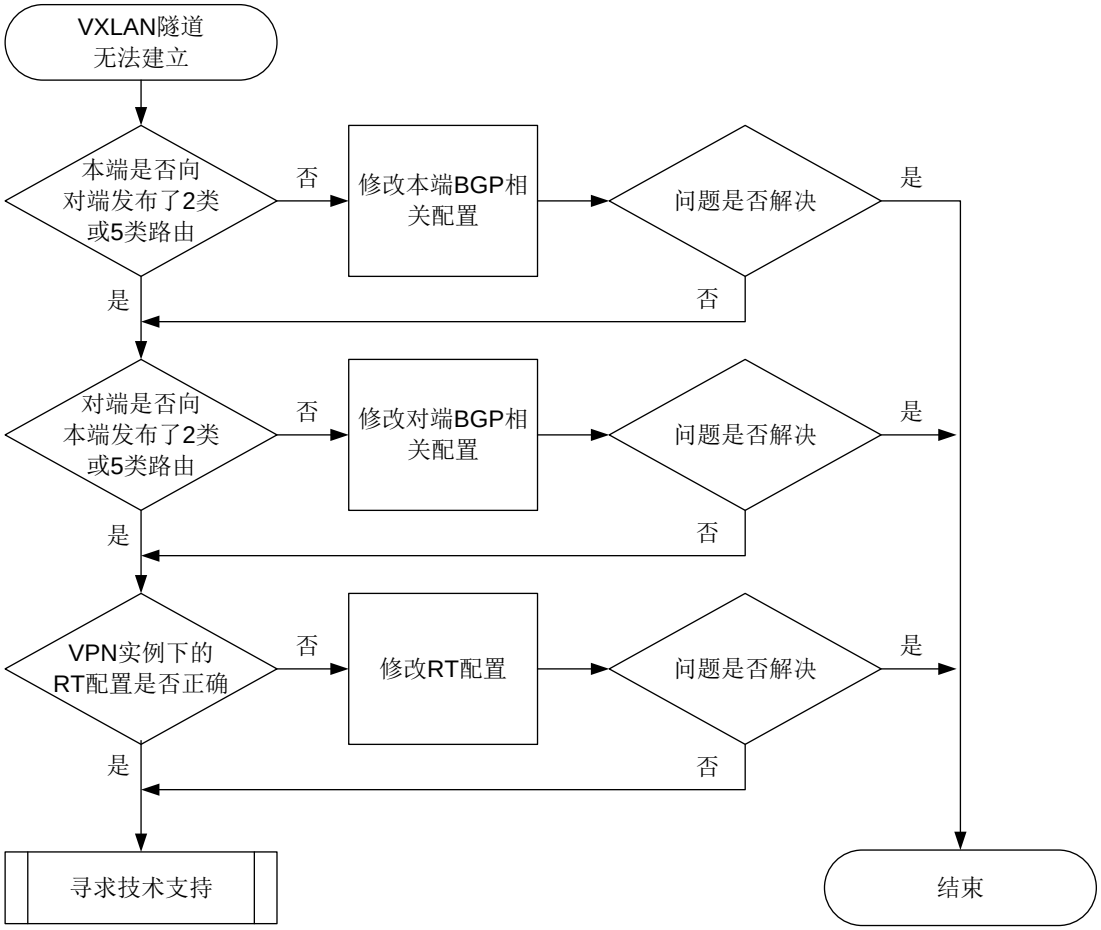
(1) 检查是否收到 2 类路由。

(2) 检查是否收到 5 类路由

(3) 检查 VPN 实例下的 RT 是否配置错误。

不同 VXLAN 内 VTEP 之间的 VXLAN 隧道无法建立的故障诊断流程如图 91 所示。

图91 不同 VXLAN 内 VTEP 之间的 VXLAN 隧道无法建立的故障诊断流程图



4. 处理步骤

不同 VXLAN 内 VTEP 之间的 VXLAN 隧道无法建立时，故障处理步骤如下：

(1) 在本端执行 **display bgp l2vpn evpn** 命令查看本端是否向对端发布了 2 类或 5 类路由。例如，下面的显示信息表示本端向 4.4.4.4 通告了 2 类和 5 类路由。如果组网中存在 RR，则 **display bgp l2vpn evpn** 命令需要指定 RR 的地址；否则，需要指定对端的地址。

```
<Sysname> display bgp l2vpn evpn peer 4.4.4.4 advertised-routes

 Total number of routes: 3

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external,
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 1:1
 Total number of routes: 1

     Network            NextHop         MED        LocPrf             Path/Ogn
```

```
* >  [5][0][24][10.1.1.0]/80
                      0.0.0.0         0          100              i

 Route distinguisher: 2:2
 Total number of routes: 2

     Network            NextHop         MED        LocPrf             Path/Ogn

* >  [2][0][48][0e86-19b6-0308][0][0.0.0.0]/104
                      0.0.0.0         0          100              i
* >  [3][0][32][1.1.1.1]/80
                      0.0.0.0         0          100              i
```

- 如果本端向对端发布了 2 类或 5 类路由，则执行第(2)步。
- 如果本端未向对端发布 2 类和 5 类路由，请检查 EVPN 功能中 BGP 的相关配置是否正确，具体配置参见“EVPN 配置指导”中的“EVPN VXLAN”。

(2) 在对端执行 **display bgp l2vpn evpn** 命令查看对端是否向本端发布了 2 类或 5 类路由。例如，下面的显示信息表示对端向 4.4.4.4 通告了 2 类和 5 类路由。如果组网中存在 RR，则 **display bgp l2vpn evpn** 命令需要指定 RR 的地址；否则，需要指定对端的地址。

```
<Sysname> display bgp l2vpn evpn peer 4.4.4.4 advertised-routes

 Total number of routes: 3

 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external,
               a - additional-path
               Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 1:1
 Total number of routes: 2

     Network            NextHop         MED        LocPrf             Path/Ogn

* >  [2][0][48][0e86-23cf-0507][0][0.0.0.0]/104
                      0.0.0.0         0          100              i
* >  [3][0][32][3.3.3.3]/80
                      0.0.0.0         0          100              i

 Route distinguisher: 3:3
 Total number of routes: 2

     Network            NextHop         MED        LocPrf             Path/Ogn

* >  [5][0][24][10.1.1.0]/80
                      0.0.0.0         0          100              i
```

- 如果对端向本端发布了 2 类或 5 类路由，则执行第(3)步。

- 如果对端未向本端发布 2 类和 5 类路由，请检查 EVPN 功能中 BGP 的相关配置是否正确，具体配置参见“EVPN 配置指导”中的“EVPN VXLAN”。

(3) 在关联 L3VNI 的 VPN 实例视图下执行 **display this** 命令查看两端的 Export target 属性与 Import target 属性配置是否正确。

```
[Sysname-vpn-instance-vpna] display this
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
return
```

- 如果两端的 RT 属性不匹配，请执行 **vpn-target** 命令修改 Route Target 属性配置。
- 如果两端的 RT 属性匹配，则执行第(4)步。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

无。

14.1.3 VXLAN 网络中，二层 VXLAN 业务流量不通

1. 故障描述

VXLAN 网络中，二层 VXLAN 业务流量不通。

2. 常见原因

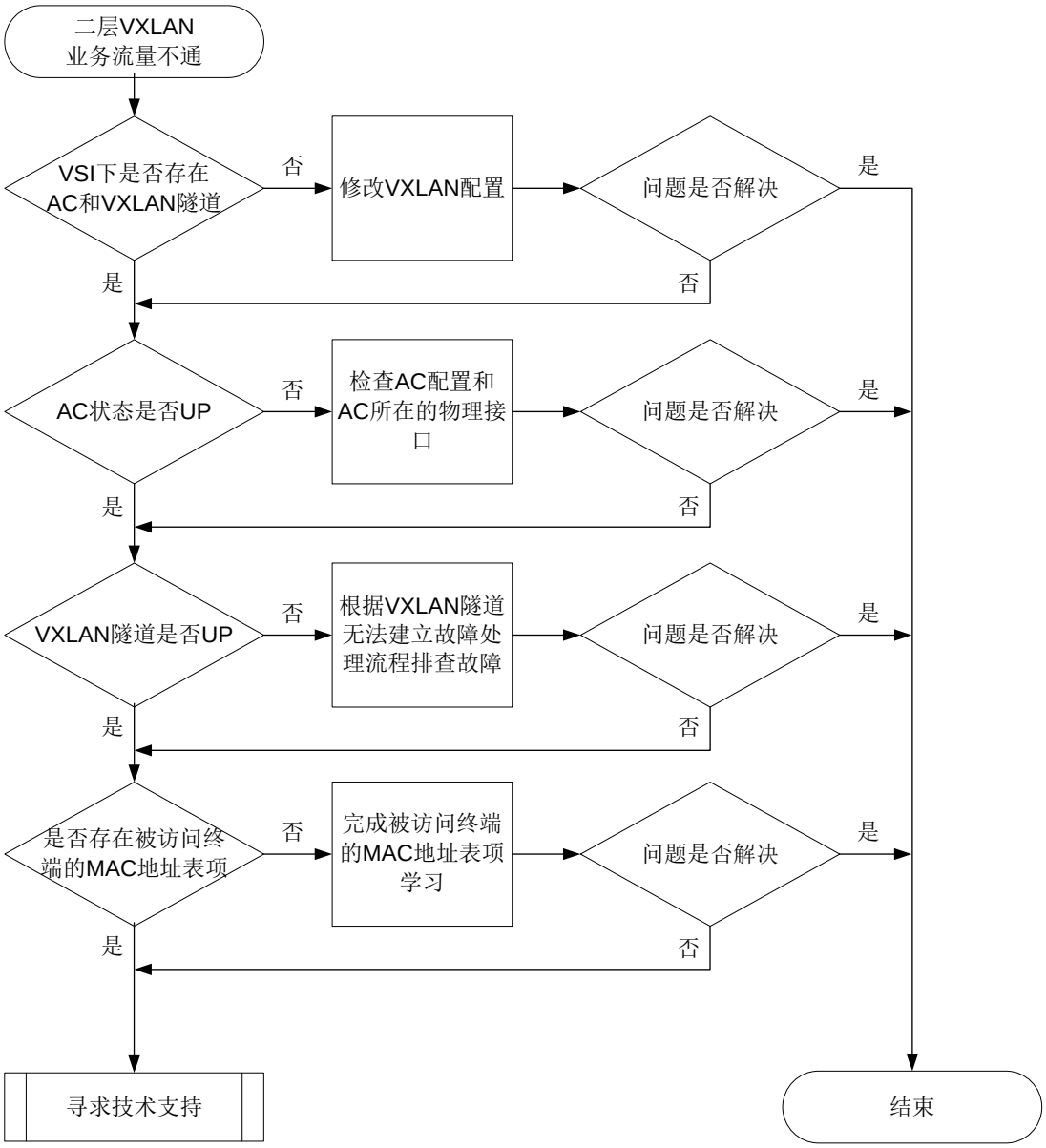
本类故障的常见原因主要包括：

- AC 或 VXLAN 隧道未建立。
- 未学习到 MAC 地址。

3. 故障分析

本类故障的诊断流程如图 92 所示。

图92 二层 VXLAN 业务流量不通的故障诊断流程图



4. 处理步骤

二层 VXLAN 业务流量不通时，故障处理步骤如下：

(1) 通过 **display l2vpn vsi verbose** 命令查看 VSI 关联的 VXLAN 隧道和 AC 信息。

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
...
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State  Type      Flood proxy
```

```
    Tunnel1              0x5000001  Up     Manual    Disabled
  ACs:
    AC                              Link ID    State     Type
    GE1/0/1 srv1000                 0          Up        Manual
```

- 若 AC 和 VXLAN 隧道均为 Up 状态，则执行第(2)步。
- 若 AC 为 Down 状态，请检查并修改 AC 配置。
- 若 VXLAN 隧道为 Down 状态，请根据“14.1.1 EVPN 分布式网关场景，同一 VXLAN 内的 VTEP 之间隧道无法建立”故障处理步骤解决问题。

(2) 通过 **display l2vpn mac-address** 命令查看 VSI 的 MAC 地址表中是否存在被访问终端的 MAC 地址表项和学习的 MAC 地址表项总数。

```
<Sysname> display l2vpn mac-address
* - The output interface is issued to another VSI
MAC Address    State     VSI Name                        Link ID/Name   Aging
0001-0001-0001 Static    aaa                             Tunnel1        NotAging
...
```

- 若存在指定的 MAC 地址表项，则执行第(3)步。
- 若不存在指定的 MAC 地址表项，请在 VSI 视图下执行 **display this** 命令，查看当前 VSI 下是否配置了 **mac-table limit** 命令和 **mac-table limit drop-unknown** 命令，如果配置了上述命令且当前已经学习到的 MAC 地址已经达到最大值，则需要将允许 VSI 学习到的最大 MAC 地址数调大或删除 **mac-table limit drop-unknown** 命令。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

无。

14.1.4 VXLAN 网络中，三层 VXLAN 业务流量不通

1. 故障描述

VXLAN 网络中，三层 VXLAN 业务流量不通。

2. 常见原因

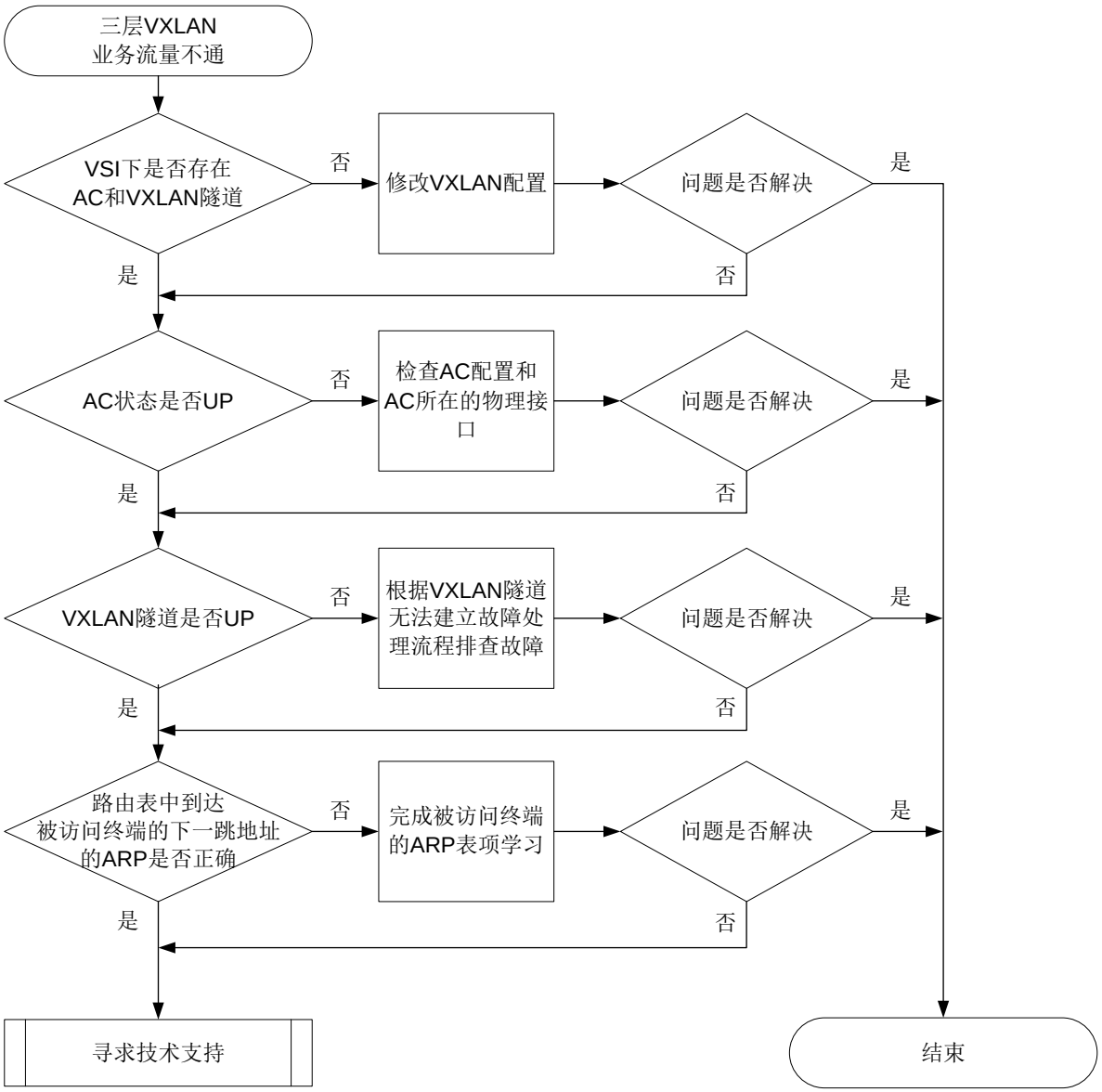
本类故障的常见原因主要包括：

- AC 或 VXLAN 隧道未建立。
- 设备的 Route MAC 配置错误。

3. 故障分析

本类故障的诊断流程如图 93 所示。

图93 三层 VXLAN 业务流量不通的故障诊断流程图



4. 处理步骤

三层 VXLAN 业务流量不通时，故障处理步骤如下：

(1) 通过 **display l2vpn vsi verbose** 命令查看 VSI 关联的 VXLAN 隧道和 AC 信息。

```
<Sysname> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
...
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State  Type      Flood proxy
```

```
    Tunnel1              0x5000001  Up     Manual    Disabled
  ACs:
    AC                              Link ID    State     Type
    GE1/0/1 srv1000                 0          Up        Manual
```

- 若 AC 和 VXLAN 隧道均为 Up 状态，则执行第(2)步。
- 若 AC 为 Down 状态，请检查并修改 AC 配置。
- 若 VXLAN 隧道为 Down 状态，请根据“14.1.2 EVPN 分布式网关场景，不同 VXLAN 内的 VTEP 之间隧道无法建立”故障处理步骤解决问题。

(2) 通过 **display evpn routing-table** 命令查看 L3VNI 关联的 VPN 实例的路由表中目的 IP 地址（IP address）为被访问终端的 IP 地址的路由表项的下一跳地址（Nexthop）。

```
<Sysname> display evpn routing-table vpn-instance vpn1
Flags: E - with valid ESI   A – A-D ready   L - Local ES exists

VPN instance name: vpn1                              Local L3VNI: 7
IP address       Nexthop          Outgoing interface    NibID       Flags
10.1.1.11        1.1.1.1          Vsi-interface3        0x18000000  EAL
```

(3) 通过 **display arp** 命令查看下一跳地址的 ARP 信息。

```
<Sysname> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
1.1.1.1         00e0-fe50-6503 vsi1          Tunnel1                  960   D
```

- 若下一跳地址对应的 MAC 地址为 Router MAC，则执行第(4)步。通过 **display interface vsi-interface** 命令查看承载 L3VNI 的 VSI 虚接口的 MAC 地址，该地址就是 Router MAC 地址。
- 若下一跳地址对应的 MAC 地址不是 Router MAC，则将设备上承载 L3VNI 的 VSI 虚接口的 MAC 地址配置一致或通过 **evpn global-mac** 命令配置 EVPN 的全局 MAC 地址。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

无。

14.1.5 EVPN 网络中，VM 迁移时间过长

1. 故障描述

EVPN 网络中，VM 迁移到新的 VTEP 后，VTEP 没有立刻学习到 VM 的 MAC 地址或者 ARP。

2. 常见原因

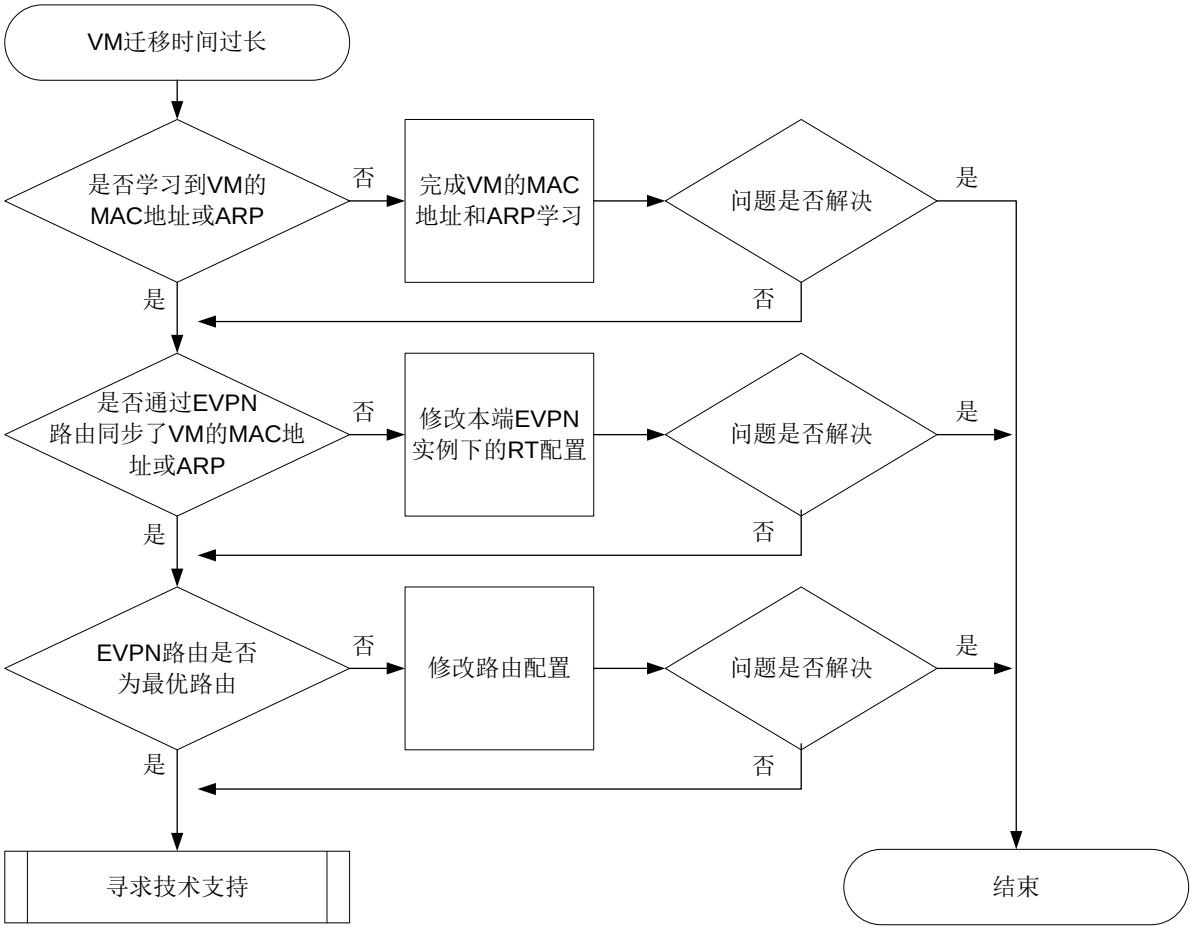
本类故障的常见原因主要包括：

- 新的 VTEP 未学习到迁移 VM 的 MAC 地址表项和 ARP 表项。
- 新的 VTEP 未通过 BGP EVPN 路由同步学习到迁移 VM 的 MAC 地址和 ARP。
- VTEP 之间同步的 BGP EVPN 路由不是最优路由。

3. 故障分析

本类故障的诊断流程如图 94 所示。

图94 VM 迁移时间过长的故障诊断流程图



4. 处理步骤

(1) 在迁移后的 VTEP 设备上查看是否学习到迁移 VM 的 MAC 地址或 ARP。

通过 **display l2vpn mac-address** 命令查看 VSI 的 MAC 地址表中是否存在迁移 VM 的 MAC 地址表项。

```
<Sysname> display l2vpn mac-address
* - The output interface is issued to another VSI
MAC Address    State     VSI Name                        Link ID/Name   Aging
52f6-bc1e-0d06 EVPN      aaa                             Tunnel10       NotAging
...
```

通过 **display arp** 命令查看 VSI 的 ARP 表项中是否包含 VM 的 ARP 表项。

```
<Sysname> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
```

```
IP address      MAC address    VLAN/VSI name Interface                Aging Type
1.1.1.4         00e0-fe60-5000 vsi2          Tunnel1                  --    M
...
```

- 若存在迁移 VM 的 MAC 地址或 ARP 表项，则执行第(2)步。
- 若不存在迁移 VM 的 MAC 地址和 ARP 表项，则表示本端未学习到迁移 VM 的 MAC 地址和 ARP，需要 VM 在迁移后的 VTEP 上上线完成 VM 的 MAC 地址和 ARP 表项学习。

(2) 在迁移前的 VTEP 设备上查看是否通过 BGP EVPN 路由同步学习到迁移 VM 的 MAC 地址或 ARP。

通过 **display evpn route mac** 命令查看是否通过 BGP EVPN 路由同步学习到迁移 VM 的 MAC 地址。Flags 中的 B 表示存在通过 BGP EVPN 路由学习的 MAC 表项。

```
<Sysname> display evpn route mac
Flags: D - Dynamic   B - BGP      L - Local active
       G - Gateway   S - Static   M - Mapping        I - Invalid

VSI name: bbb
EVPN instance: -
MAC address     Link ID/Name   Flags   Encap          Next hop
0000-0000-000a  1              DL      VXLAN          -
0001-0001-0001  Tunnel1        B       VXLAN          2.2.2.2
```

通过 **display evpn route arp** 命令查看是否通过 BGP EVPN 路由同步学习到迁移 VM 的 ARP 信息。Flags 中的 B 表示存在通过 BGP EVPN 路由学习的 ARP 表项。

```
<Sysname> display evpn route arp
Flags: D - Dynamic   B - BGP      L - Local active
       G - Gateway   S - Static   M - Mapping        I - Invalid

VPN instance: vpn1                          Interface: Vsi-interface1
IP address      MAC address     Router MAC      VSI index   Flags
10.1.1.1        0001-0001-0001  a0ce-7e40-0400  0           B
10.1.1.11       0001-0001-0002  a0ce-7e40-0400  0           DL
10.1.1.101      0001-0011-0101  a0ce-7e40-0400  0           SL
10.1.1.102      0001-0011-0102  0011-9999-0000  0           BS
```

- 若通过 BGP EVPN 路由同步学习到迁移 VM 的 MAC 地址或 ARP，则执行第(3)步。
- 若未通过 BGP EVPN 路由同步学习到迁移 VM 的 MAC 地址和 ARP，请通过 **vpn-target** 命令修改本端 EVPN 实例下的 RT 配置，保证本端和对端 EVPN 实例下的 RT 属性匹配。

(3) 通过 **display bgp l2vpn evpn** 命令查看 VM 的 MAC 地址和 ARP 信息的 MAC/IP 发布路由是否为最优路由，即检查显示信息的 State 字段取值是否包括 best。如下举例中，路由通告的 MAC 地址为 0001-0203-0405（MAC address），IP 地址为 5.5.5.5/32（IP address），且该路由为 best 路由（State）。

```
<Sysname> display bgp l2vpn evpn route-distinguisher 1.1.1.1:100
[2][5][48][0001-0203-0405][32][5.5.5.5] 136

 BGP local router ID: 172.16.250.133
 Local AS number: 100


 Route distinguisher: 1.1.1.1:100
```

```
Total number of routes: 1
Paths:   1 available, 1 best

BGP routing table information of [2][5][48][0001-0203-0405][32][5.5.5.5]/136:
From            : 10.1.1.2 (192.168.56.17)
Rely nexthop    : 10.1.1.2
Original nexthop: 10.1.1.2
OutLabel        : NULL
Ext-Community   : <RT: 1:2>, <RT: 1:3>, <RT: 1:4>, <RT: 1:5>, <RT: 1:6>, <RT: 1:7
                  >, <Encapsulation Type: VXLAN>, <Router's Mac: 0006-0708-0910
                  >, <MAC Mobility: Flag 0, SeqNum 2>, <Default GateWay>
RxPathID        : 0x0
TxPathID        : 0x0
AS-path         : 200
Origin          : igp
Attribute value : MED 0, pref-val 0
State           : valid, external, best
IP precedence   : N/A
QoS local ID    : N/A
Traffic index   : N/A
EVPN route type : MAC/IP advertisement route
ESI             : 0001.0203.0405.0607.0809
Ethernet tag ID : 5
MAC address     : 0001-0001-0001
IP address      : 10.1.1.1/32
MPLS label1     : 10
MPLS label2     : 100
Re-origination  : Enable
```

- 若 MAC/IP 发布路由是最优路由，则执行第(4)步。
- 若 MAC/IP 发布路由不是最优路由，请修改路由配置，确保通告的 MAC/IP 发布路由为最优路由。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

无。

14.1.6 VXLAN DCI 隧道未成功建立

1. 故障描述

VXLAN DCI 隧道未成功建立。

2. 常见原因

本类故障的常见原因为：未开启接口的 DCI 功能。

3. 故障分析

本类故障的诊断思路为：检查 ED 间互连的三层接口上是否开启 DCI 功能。

4. 处理步骤

(1) 检查 ED 间互连的三层接口（三层以太网接口及其子接口、三层以太网聚合接口及其子接口、VLAN 接口）上是否配置了 **dci enable** 命令。若未配置，则执行 **dci enable** 命令，开启接口的 DCI 功能。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 使用 **display diagnostic-information** 命令收集诊断信息。

5. 告警与日志

相关告警

无。

相关日志

无。

15 ACL 和 QoS 故障处理

15.1 QoS故障处理

15.1.1 流量不匹配分类的定位思路

1. 故障描述

执行 **display qos policy interface** 命令查看指定接口上 QoS 策略的配置信息和运行情况时，发现当前接口上的流量未匹配到 QoS 策略中的流分类规则。

对于硬件转发产品，如下显示信息指定的流分类 1 中 Accounting enable 字段为 0 (Bytes/Packets) 0 (bps)，表示接口上符合流分类规则的数据包数目为 0。需要注意的是，如果在硬件转发产品上希望看到上述符合流分类规则的统计信息，需要在 QoS 策略的流行为中执行 **accounting** 命令来配置流量统计动作。

对于软件转发产品，如下显示信息指定的流分类 1 中 Matched 字段为 0 (Packets) 0 (Bytes)，表示接口上符合流分类规则的数据包数目为 0。需要注意的是，软件转发产品的 QoS 策略中默认存在名称为 default-class 的流分类，未匹配到 QoS 策略中其他流分类规则的流量均匹配 default-class 的流分类。

```
<Sysname> display qos policy interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: default-class
     Matched : 213126 (Packets) 40928738 (Bytes)
```

```
    5-minute statistics:
     Forwarded: 20/4208 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match any
    Behavior: be
     -none-
  Classifier: 1
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match acl 3000
    Behavior: 1
     Marking:
       Remark dscp 3
```

2. 常见原因

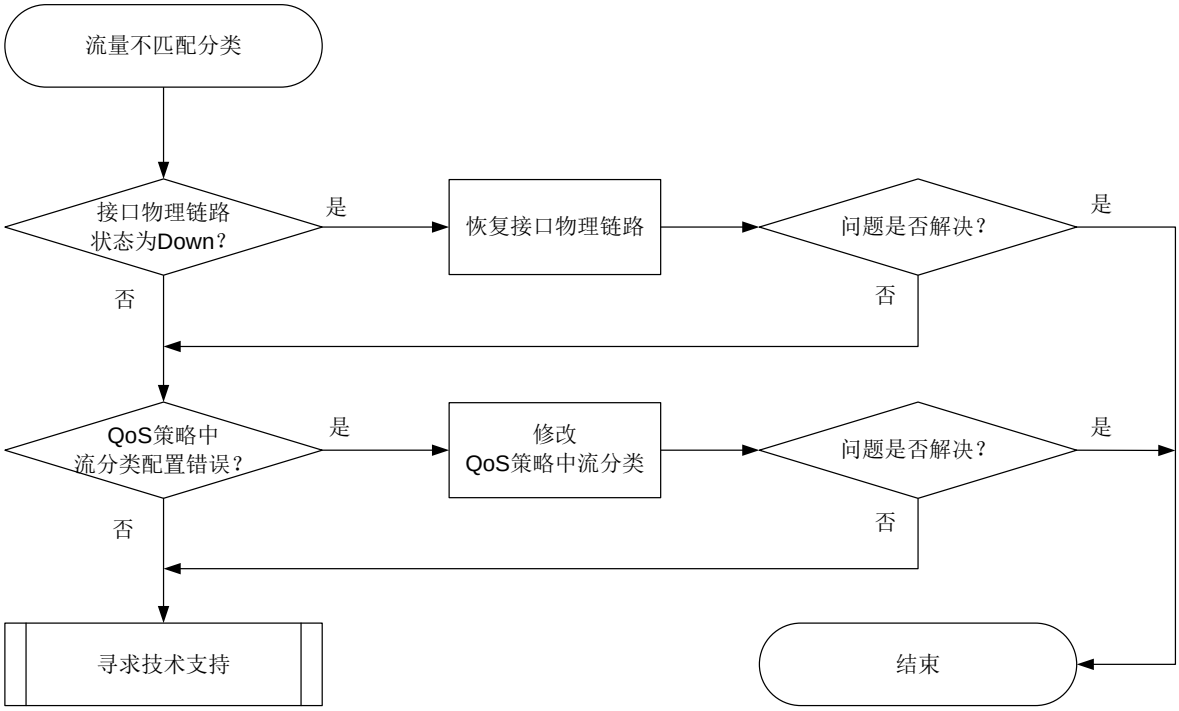
本类故障的常见原因主要包括：

- 应用了QoS策略的接口状态为Down，没有转发流量。
- 流分类配置错误，不能匹配到转发流量。
- 流分类中ACL规则匹配的流量执行了更高优先的策略。

3. 故障诊断流程

本类故障的诊断流程如图 95 所示。

图95 流量不匹配分类的故障诊断流程图



4. 故障处理步骤

(1) 检查接口物理链路状态是否正常。

在设备上执行 **display interface** 命令检查接口状态，例如：

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Interface index: 386
Current state: Administratively DOWN
Line protocol state: DOWN
…
```

a. 如果 Current state 显示为 Administratively DOWN，则在接口下执行 **undo shutdown** 命令打开关闭的接口。

b. 如果 Current state 显示为 DOWN，则检查接口的物理连线。

c. 如果接口物理链路正常，问题仍未解决，则请继续执行以下操作。

(2) 检查设备接口下应用的 QoS 策略中的流分类配置。

在设备上执行 **display traffic classifier user-defined** 命令检查用户定义的流分类的配置信息，关于 **if-match** 命令的匹配规则详细信息，请参见“ACL 和 QoS 命令参考”中的“QoS”。

如果流分类的配置错误，则执行 **traffic classifier** 命令进入该流分类视图，并执行 **if-match** 命令修改流分类的匹配规则。例如：

```
[Sysname-classifier-1] if-match dscp ef
[Sysname-classifier-1] display this

traffic classifier a operator or
```

```
 if-match protocol ipv6
 if-match dscp ef
```

请确认 Operator 字段显示的各规则之间的逻辑关系是否准确。AND 表示该流分类下的规则之间是逻辑与的关系，即数据包必须匹配全部规则才属于该类。OR 表示该流分类下的规则之间是逻辑或的关系，即数据包匹配任一规则均属于该类。本例中，如果 Rule(s)中流分类规则不止一条，且 Operator 显示字段为 AND，则表示该流分类下的规则之间是逻辑与的关系，即数据包必须匹配全部规则才属于该类。此时，请执行 **traffic classifier** 命令指定 **operator** 参数为 **or**。

```
<Sysname> display traffic classifier user-defined

  User-defined classifier information:

   Classifier: 1 (ID 101)
     Operator: AND
     Rule(s) :
      If-match dscp ef


   Classifier: 2 (ID 102)
     Operator: AND
     Rule(s) :
      If-match dscp af21


   Classifier: 3 (ID 103)
     Operator: AND
     Rule(s) :
      If-match dscp af11
```

如果 QoS 策略中的流分类配置正确，问题仍未解决，则请继续执行以下操作。

(3) 当流分类中引用 ACL 规则进行流量报文匹配时，也可能由于该 ACL 规则匹配到的流量报文执行了其他更高优先的策略行为导致 MQC 方式配置的 QoS 策略未生效，不同策略行为的优先顺序为：

在报文出方向：报文过滤>全局应用 MQC 方式配置的 QoS 策略>接口应用 MQC 方式配置的 QoS 策略。

在报文入方向：报文过滤>接口应用 MQC 方式配置的 QoS 策略>全局应用 MQC 方式配置的 QoS 策略。

请执行 **display current-configuration** 命令检查当前生效的配置中是否存在上述更高优先级的策略行为相关配置。如果不存在相关配置，问题仍未解决，请继续执行以下操作。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息。

5. 告警与日志

相关告警

无

相关日志

- QOS_POLICY_APPLYIF_CBFAIL
- QOS_POLICY_APPLYIF_FAIL

16 用户接入与认证故障处理

16.1 802.1X故障处理

16.1.1 802.1X 用户认证失败

1. 故障描述

802.1X 用户认证失败或认证异常。

2. 常见原因

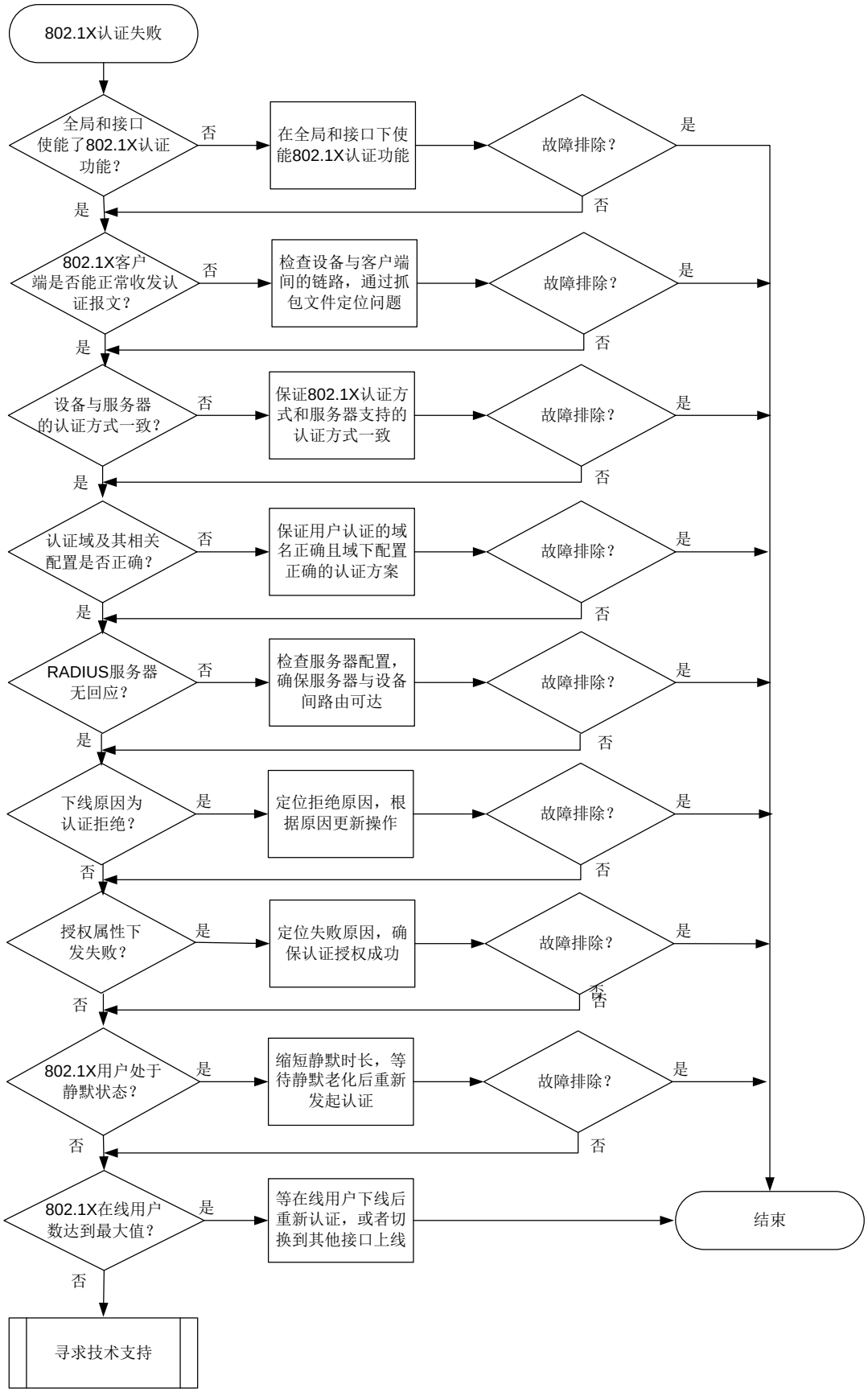
本类故障的常见原因主要包括：

- 全局或接口 802.1X 功能未开启。
- 802.1X 客户端不能正常发送或接收认证报文。
- 设备配置的认证方式与 RADIUS 服务器不一致。
- 802.1X 用户使用的认证域及相关配置错误。
- RADIUS 服务器无回应。
- RADIUS 服务器认证拒绝。
- 授权属性下发失败。
- 802.1X 用户处于静默状态。
- 802.1X 在线用户数达到最大值。

3. 故障分析

本类故障的诊断流程如图 96 所示。

图96 802.1X 用户认证失败的故障诊断流程图



4. 处理步骤

注意

- Debug 开关不能在设备正常运行时随意开启，可在故障发生后复现故障场景时打开。
- 请及时保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

(1) 检查设备全局或接口 802.1X 功能是否开启。

通过在设备上执行 **display dot1x** 命令，检查全局和认证接口上的 802.1X 功能是否开启。

- 如果提示“802.1X is not configured.”，表示全局 802.1X 功能未开启，请在系统视图下执行 **dot1x** 命令，开启全局 802.1X 认证功能。
- 如果有全局配置信息，无接口下的配置信息显示，则说明接口下未开启 802.1X 功能，请在认证接口视图下执行 **dot1x** 命令。

(2) 检查 802.1X 客户端是否能正常发送或接收认证报文。

- 检查 802.1X 客户端版本是否为设备和服务器支持的版本。
- 检查设备与 802.1X 客户端间的链路连接是否正常。
- 通过抓包检查设备与客户端间是否能正常收发数据报文，分析抓包文件进一步定位故障问题。

(3) 检查设备上配置的认证方法与 RADIUS 服务器是否一致。

设备上 802.1X 系统支持两种认证方法：EAP 终结（PAP 和 CHAP）和 EAP 中继（EAP），配置 EAP 认证方法时需要注意以下几点：

- 保证设备和 RADIUS 服务器配置的认证方法一致，且客户端支持。
- 本地认证仅支持 EAP 终结方式。

通过在设备上执行 **display dot1x** 命令查看当前 802.1X 采用的认证方式。

```
<Sysname> display dot1x
 Global 802.1X parameters:
   802.1X authentication                       : Enabled
   EAP authentication                          : Enabled
...
```

如果与服务器不一致，可通过 **dot1x authentication-method** 命令修改。

(4) 检查认证域及相关配置是否正确。

802.1X 用户按照如下先后顺序选择认证域：端口上指定的强制 ISP 域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。

a. 通过在设备上执行 **display dot1x** 命令查看认证接口下是否配置了 802.1X 用户的强制认证域。

```
<Sysname> display dot1x
...
 GigabitEthernet1/0/1  is link-up
   802.1X authentication                       : Enabled
...
   Multicast trigger                           : Enabled
```

```
   Mandatory auth domain                       : Not configured
```

...

如果配置了强制认证域，请执行 **display domain** 命令检查强制认证域下的认证方案是否配置准确。

b. 如果没有配置强制认证域，若 802.1X 用户名中包含域名，请确认域名分隔符与 RADIUS 服务器支持的域名分隔符保持一致，然后根据用户名中包含的域名找到指定域并检查其配置。

c. 如果 802.1X 用户名中未包含域名，则检查缺省认证域的配置。

d. 如果不存在缺省认证域，若通过 **domain if-unknown** 命令配置了 unknown 域，则检查 unknown 域下的认证方案是否配置准确。

e. 如果根据以上原则决定的认证域在设备上都不存在，则用户无法完成认证。

(5) 检查 RADIUS 服务器有无响应。

具体的故障定位操作请参见《AAA 故障处理手册》的“RADIUS 服务器无响应”。

(6) 检查下线原因是否为认证拒绝。

RADIUS 服务器认证拒绝有多种原因，最常见的有服务器上未添加用户名、用户名密码错误、RADIUS 服务器授权策略无法匹配等。通过执行 **debugging radius error** 命令打开 RADIUS 错误调试信息开关查看相关的 Debug 信息，并且同时可以在设备上执行 **test-aaa** 命令发起 RADIUS 请求测试，定位故障问题后，调整服务器、设备及客户端配置。

(7) 检查授权属性是否下发失败。

a. 检查设备上是否通过 **port-security authorization-fail offline** 命令配置了授权失败用户下线功能。如果未配置授权失败用户下线功能，缺省情况下授权失败用户也可以保持在线，则用户不是因为授权失败而导致认证失败，继续定位其它故障原因。

b. 如果配置了授权失败用户下线功能，则可以通过打印的“DOT1X_LOGIN_FAILURE”日志确认授权失败的属性（例如授权 ACL、VLAN）。

c. 检查服务器上的授权属性（例如授权 ACL、VLAN）设置是否正确，确保服务器下发的授权属性内容准确。

d. 执行 **display acl** 或 **display vlan** 命令检查设备上对应的授权属性是否存在，如果不存在，需要在设备上创建相应的授权属性，确保用户能够获取到授权的信息。

(8) 检查 802.1X 用户是否处于静默状态。

在设备上执行 **display dot1x** 命令，显示信息中“Quiet timer”和“Quiet period”字段显示的是静默定时器的开启状态和静默时长，“Online 802.1X users”字段下如果用户的“Auth state”显示为“Unauthenticated”时，则表示该用户为 802.1X 静默用户。

静默期间，设备将不对静默用户进行 802.1X 认证处理。用户需等待静默时间老化后，重新发起 802.1X 认证，同时也可通过执行 **dot1x timer quiet-period** 命令重新设置静默时长。

(9) 检查 802.1X 在线用户数是否达到最大值。

a. 在设备上执行 **display dot1x interface** 查看认证接口下的信息，“Max online users”字段为该接口下配置的最大用户数，“Online 802.1X users”字段为接口下当前在线用户数，对比两组数据判断 802.1X 认证在线用户数是否已经达到最大值。

b. 如果接口接入的 802.1X 用户数达到最大值，可以通过 **dot1x max-user** 命令增大最多允许同时接入的 802.1X 用户数。

c. 如果接口接入的 802.1X 用户数无法再增加，则需要等其他用户下线或切换用户的接入端口。

(10) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 执行 **debugging dot1x all**、**debugging radius all** 命令收集的调试信息。

5. 告警与日志

相关告警

无

相关日志

- DOT1X_LOGIN_FAILURE

16.1.2 802.1X 用户掉线

1. 故障描述

802.1X 用户认证成功上线后，异常掉线。

2. 常见原因

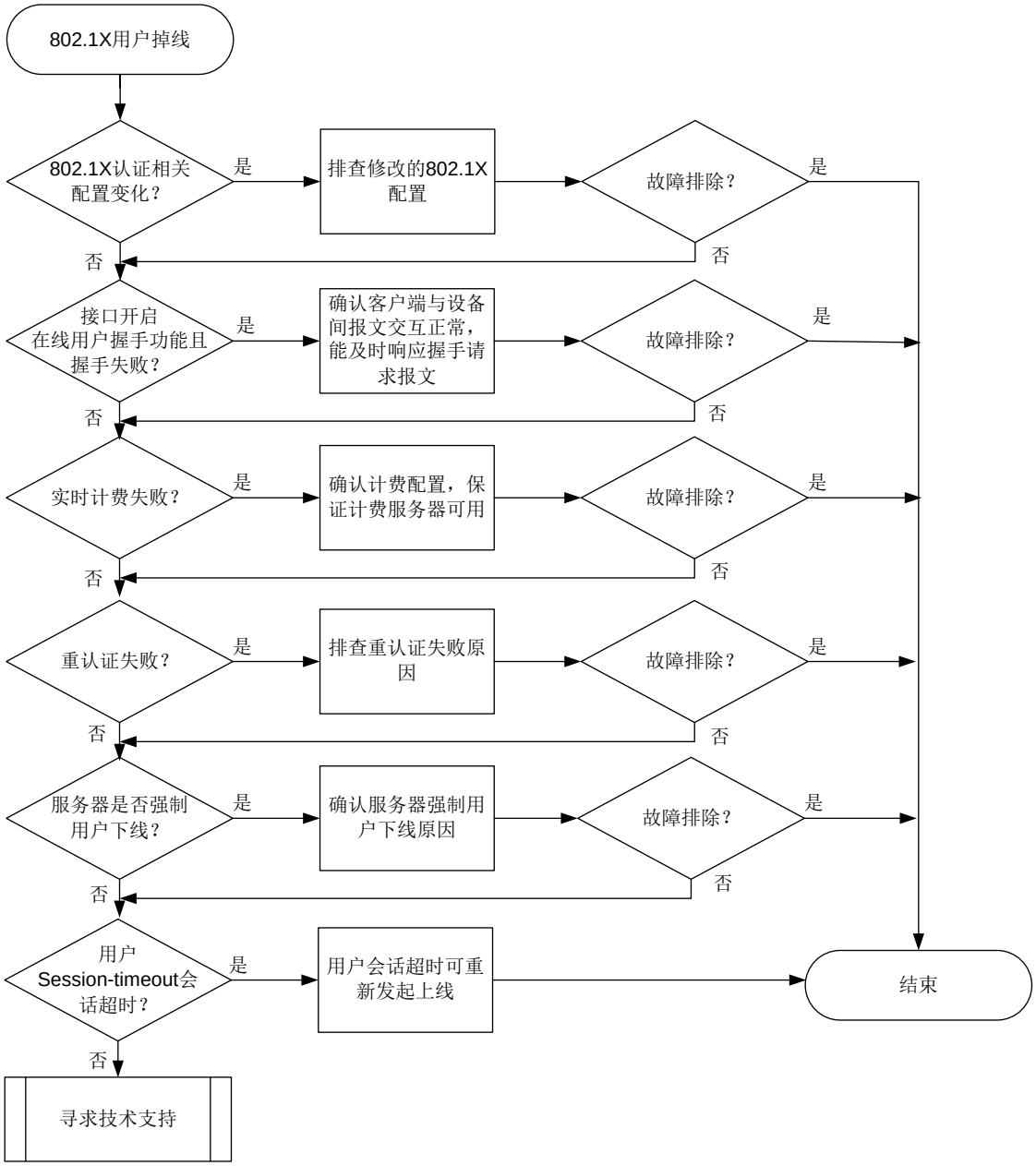
本类故障的常见原因主要包括：

- 设备上 802.1X 认证的相关配置变化。
- 在线用户握手失败。
- 实时计费失败。
- 802.1X 用户重认证失败
- 服务器强制用户下线。
- 用户会话超时。

3. 故障分析

本类故障的诊断流程如图图 97 所示。

图97 802.1X 用户掉线的故障诊断流程图



4. 处理步骤

注意

- Debug 开关不能在设备正常运行时随意开启，可在故障发生后复现故障场景时打开。
- 请及时保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

(1) 检查设备上 802.1X 认证的相关配置是否发生变化。

a. 通过 **display dot1x** 命令查看设备上 MAC 地址认证的相关配置是否发生变化。

b. 通过 **display domain** 命令查看用户认证域下的配置是否发生变化。

(2) 检查 802.1X 在线用户握手交互是否失败。

a. 执行 **display dot1x** 命令通过“Handshake”字段查看认证接口下是否开启了 802.1X 在线用户握手功能。

b. 通过“DOT1X_LOGOFF”日志确认用户失败的原因为握手失败。可以通过抓包检查设备与客户端间是否能正常收发 EAP 数据报文，分析抓包文件进一步定位问题。

(3) 检查实时计费是否失败。

通过“DOT1X_LOGOFF”日志确认用户失败的原因为实时计费失败。检查设备与计费服务器之间的链路状态，以及设备和服务器的相关计费配置是否发生过更改。

(4) 检查用户是否是因为重认证失败而掉线。

a. 执行 **display dot1x** 命令通过“Periodic reauth”字段查看认证接口下是否开启了 802.1X 周期性重认证功能。

b. 通过打印的“DOT1X_LOGOFF”日志确认用户异常掉线的原因为重认证失败。

c. 参考“16.1.1 802.1X 用户认证失败”故障处理定位重认证失败原因。

(5) 检查是否为 RADIUS 服务器强制用户下线。

通过打印的“DOT1X_LOGOFF”日志确认用户异常掉线的原因为 RADIUS 服务器强制用户下线。请联系服务器管理员定位服务器强制用户下线原因。

(6) 检查用户会话是否超时。

a. 检查是否配置了 802.1X 认证用户会话超时时间。

– RADIUS 远程认证情况下，执行 **debugging radius packet** 命令打开 RADIUS 报文调试信息开关，通过调试信息确认服务器回应的报文中是否携带 Session-Timeout 属性。

– 本地认证情况下，执行 **display local-user** 命令查看显示信息中是否包含“Session-timeout”字段。

b. 通过打印的“DOT1X_LOGOFF”日志确认用户异常掉线的原因为下发的用户会话超时。

c. 用户会话超时触发的掉线情况属于正常现象，用户可重新发起上线。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 执行 **debugging dot1x all**、**debugging radius all** 命令收集的调试信息。

5. 告警与日志

相关告警

无

相关日志

- DOT1X_LOGOFF

16.2 AAA故障处理

16.2.1 登录设备后无法执行部分命令行

1. 故障描述

管理员登录设备后没有部分命令行的执行权限，系统打印提示信息 “Permission denied.”。

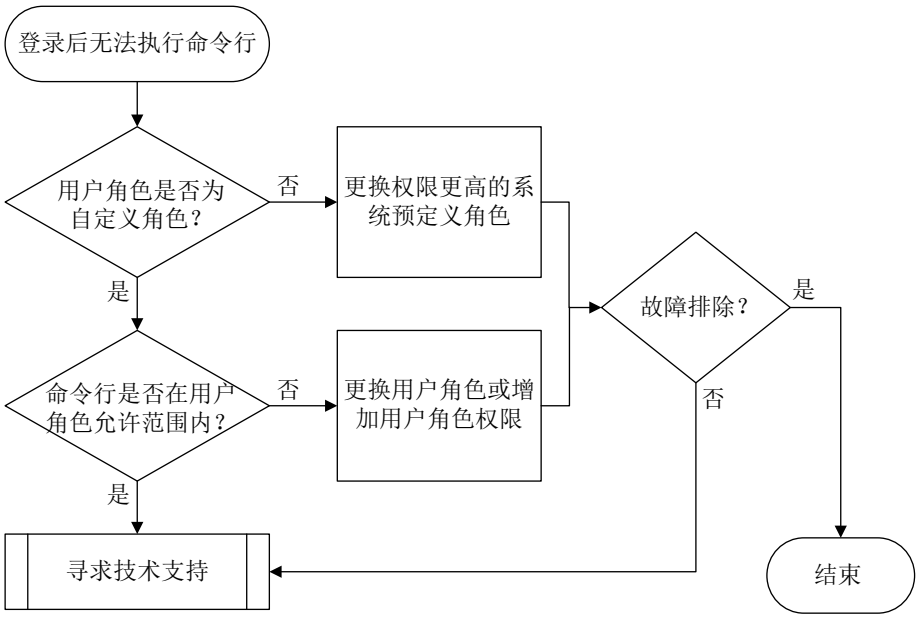
2. 常见原因

本类故障的主要原因为，给用户授权的用户角色权限过小。

3. 故障分析

本类故障的诊断流程如图 98 所示。

图98 登录后无法执行部分命令行的故障诊断流程图



4. 处理步骤

(1) 检查用户角色否为自定义用户角色。

请以超级管理员身份（即具有 network-admin、或者 level-15 用户角色）登录设备，执行 **display line** 命令查看登录用户线的认证方式，并根据不同的认证方式，采取不同的处理步骤：

```
<Sysname> display line
  Idx  Type     Tx/Rx       Modem Auth  Int          Location
  0    CON 0    9600        -     N     -            0/0
+ 81   VTY 0                 -     N     -            0/0
+ 82   VTY 1                 -     P     -            0/0
+ 83   VTY 2                 -     A     -            0/0
...
```

- 对于 none 和 password 认证方式（Auth 字段：N、P），检查对应用户线视图下的用户角色是否为自定义用户角色。如果不是自定义用户角色，则通过 **user-role** *role-name* 命令设置权限更高的系统预定义角色。
- 对于 **scheme** 认证方式（Auth 字段：A），首先查看登录用户认证域下配置的认证方法：
  - 如果采用了 Local 认证方法，则通过 **display local-user** 命令查看用户角色是否为自定义用户角色。如果不是自定义用户角色，则通过 **authorization-attribute user-role** *role-name* 命令设置权限更高的系统预定义角色（下例为 network-admin）。

    ```
    <Sysname> system-view
    [Sysname] local-user test class manage
    [Sysname-luser-manage-test] authorization-attribute user-role network-admin
    ```
  - 如果采用了远程认证方法，则联系远程认证服务器管理员，为用户授权权限更高的系统预定义角色。

(2) 检查不允许执行的命令行是否在自定义用户角色允许的权限范围内。

a. 执行命令 **display role name** *role-name*，查看用户的自定义角色拥有的命令行权限规则。

b. 如果用户所执行的命令行不在所属用户角色拥有的命令行权限范围之内，则为其更换权限较高的系统域定义用户角色，或者通过命令 **rule** 为用户的自定义角色增加对应的命令行权限规则。需要注意的是，自定义用户角色即使配置了较高的权限规则，仍然有部分无法支持的命令行，这些命令行的明细请查看“基础配置指导”中的“RBAC”手册。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.2 登录设备后无法创建或修改本地用户

1. 故障描述

管理员登录设备后无法创建或修改本地用户，系统打印提示信息“Insufficient right to perform the operation.”。

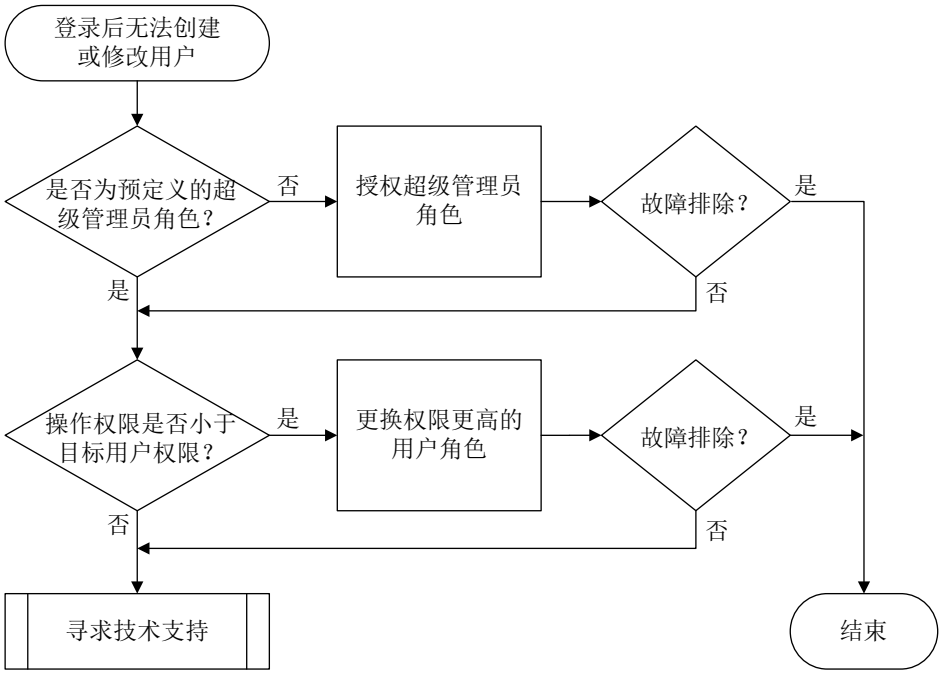
2. 常见原因

本类故障的主要原因为，给用户授权的用户角色权限不具备修改目标本地用户配置的权限。

3. 故障分析

本类故障的诊断流程如图 99 所示。

图99 登录后无法创建或修改本地用户的故障诊断流程图



4. 处理步骤

(1) 检查登录用户的角色是否为预定义的超级管理员角色，即为 network-admin、level-15、之一。

只有上述预定义用户角色才拥有创建本地用户的权限,其它用户角色只有进入自身本地用户视图的权限。如果登录用户不拥有如上预定义用户角色,则为其授权其中之一。如果重新授权后，故障仍未排除，请继续定位。

此步骤仅适用于无权限创建本地用户，若无权限修改本地用户，请执行步骤（2）。

(2) 比较登录用户和目标用户的权限范围。

执行命令 **display role name** *role-name*，分别查看登录用户和目标用户的角色权限，并比较两者的权限大小。如果操作者权限较小，则为其更换拥有更高权限的用户角色。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- LOCAL/5/LOCAL_CMDDENY

16.2.3 管理员未被授权用户角色

1. 故障描述

管理员无法成功登录设备，设备也没有提供三次登录尝试机会。例如，使用 Telnet 登录时，用户输入用户名和密码后，设备登录界面上既未打印提示信息“AAA authentication failed”，也未再次提示用户输入用户名和密码。

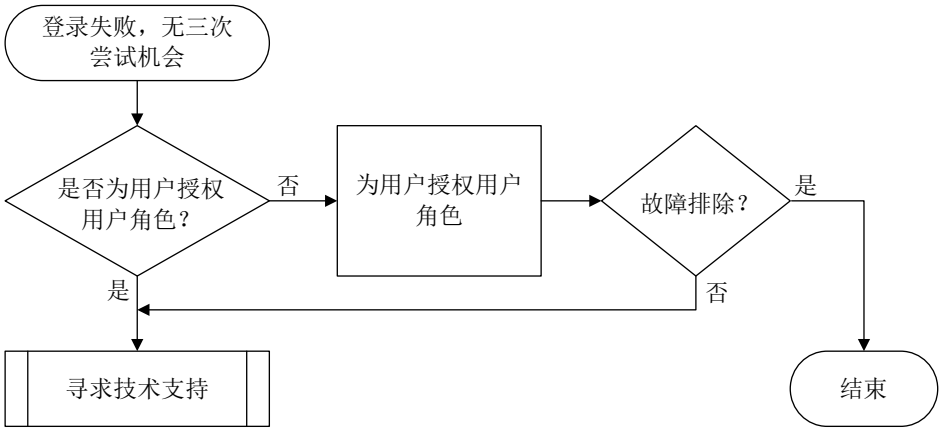
2. 常见原因

本类故障的主要原因为，没有为用户授权用户角色。

3. 故障分析

本类故障的诊断流程如图 100 所示。

图100 管理员未被授权用户角色的故障诊断流程图



4. 处理步骤

(1) 检查是否为用户授权了用户角色。

请以超级管理员身份（即具有 network-admin、或者 level-15 用户角色）登录设备，执行 **display line** 命令查看登录用户线的认证方式，并根据不同的认证方式，采取不同的处理步骤：

```
<Sysname> display line
  Idx  Type     Tx/Rx      Modem Auth  Int          Location
  0    CON 0    9600       -     N     -            0/0
+ 81   VTY 0               -     N     -            0/0
+ 82   VTY 1               -     P     -            0/0
+ 83   VTY 2               -     A     -            0/0
...
```

- 对于 none 和 password 认证方式（Auth 字段：N、P），检查对应用户线视图下是否存在用户角色配置。如果不存在，则通过 **user-role** *role-name* 命令设置用户角色（下例中为 abc）。

  ```
  <Sysname> system-view
  [Sysname] line vty 0 63
  [Sysname-line-vty0-63] user-role abc
  ```

- 对于 **scheme** 认证方式（Auth 字段：A），首先查看登录用户认证域下配置的认证方法：

– 如果采用了 Local 认证方法，则执行 **display local-user** 命令查看该用户的授权用户角色情况，如果显示信息中的“User role list：”字段为空，则表示该用户没有被授权任何用户角色。

```
<Sysname> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
  State:                     Active
  Service type:              Telnet
  User group:                system
  Bind attributes:
  Authorization attributes:
    Work directory:          flash:
    User role list:

…
```

此时，需要进入该本地用户视图，执行 **authorization-attribute user-role** 命令为用户授权角色（下例中为 abc）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] authorization-attribute user-role abc
```

– 如果采用了远程认证方法，则联系远程认证服务器管理员确认是否为该用户授权了用户角色，若无，请为该用户添加用户角色属性。以 Free RADIUS 服务器为例，如果需要在 users 文件中添加用户角色 network-admin，则需要编辑的脚本如下：

```
user  Cleartext-Password := "123456"

      H3C-User-Roles ="shell:roles=\"network-admin\""
```

其它 RADIUS 服务器上的用户角色添加方式请以实际情况为准。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.4 登录用户名含有非法字符

1. 故障描述

管理员登录设备失败，系统打印如下形式的日志信息：

```
Sysname LOGIN/5/LOGIN_INVALID_USERNAME_PWD: -MDC=1; Invalid username or password from
xx.xx.xx.xx.
```

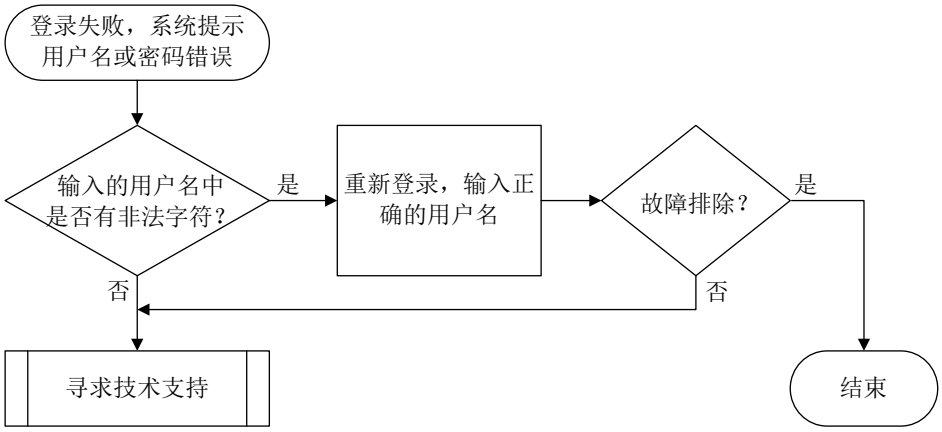
2. 常见原因

本类故障的主要原因为，用户输入的用户名中含有非法字符。

3. 故障分析

本类故障的诊断流程如图 101 所示。

图101 登录用户名含有非法字符的故障诊断流程图



4. 处理步骤

说明

本处理步骤仅适用于 SSH 及 Telnet 登录用户。

(1) 检查用户输入的用户名是否含有非法字符。

用户登录设备时，系统会检查用户输入的纯用户名以及域名的有效性，如果纯用户名中包含了非法字符“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，域名中包含“@”，则不允许登录。此时，建议用户再次尝试登录，并输入正确的用户名。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- LOGIN_INVALID_USERNAME_PWD

16.2.5 本地用户名或密码错误

1. 故障描述

管理员采用本地认证方式登录设备失败。如果设备上同时打开了 Local-Server 的事件调试信息开关（通过执行 **debugging local-server event** 命令），系统会打印如下形式的调试信息：

```
*Aug 18 10:36:58:514 2021 Sysname LOCALSER/7/EVENT: -MDC=1;
 Authentication failed, user password is wrong.
```

或者

```
*Aug 18 10:37:24:962 2021 Sysname LOCALSER/7/EVENT: -MDC=1;
 Authentication failed, user "t4" doesn't exist.
```

2. 常见原因

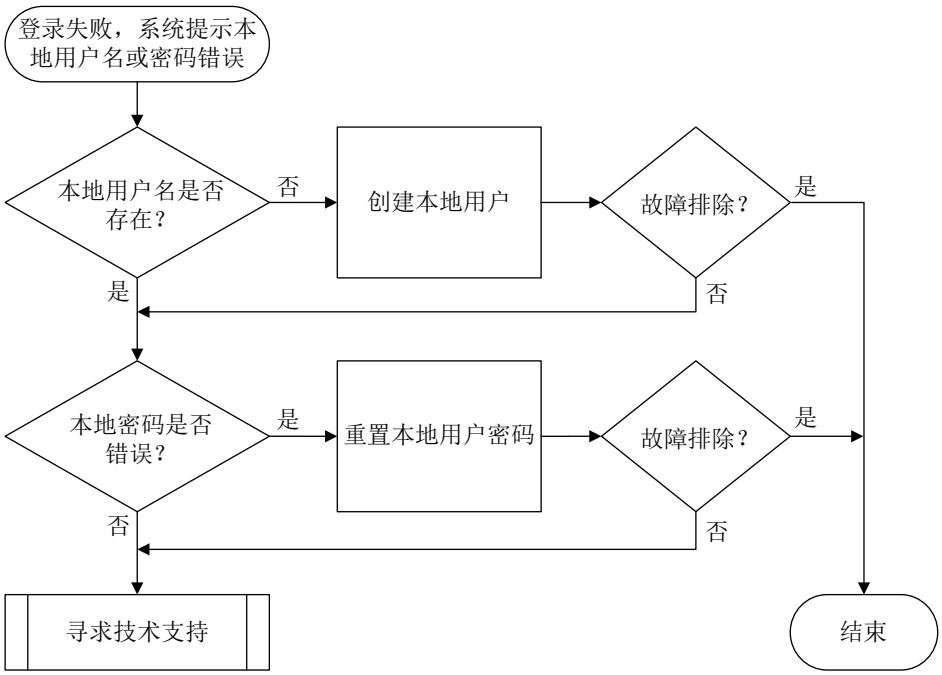
本类故障的常见原因主要包括：

- 用户输入的密码错误。
- 本地用户名不存在。

3. 故障分析

本类故障的诊断流程如图 102 所示。

图102 本地用户名或密码错误的故障诊断流程图



4. 处理步骤

(1) 检查本地用户名是否存在。

执行 **display local-user** 命令查看是否存在与登录用户名相同的设备管理类本地用户。

- 如果不存在该本地用户，则需要使用 **local-user** 命令创建设备管理类本地用户（下例中用户名为 test），并通知该用户再次尝试登录设备。

```
<Sysname> system-view
```

```
[Sysname] local-user test class manage
[Sysname-luser-manage-test]
```

- 如果存在该本地用户，请执行步骤（2）。

(2) 确认本地用户密码是否正确。

如果用户登录时系统提示密码错误，则进入对应的本地用户视图后，执行 **password** 命令重置密码（下例中为 123456TESTplat&!），并通知该用户再次尝试登录设备。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password simple 123456TESTplat&!
```

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、调试信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.6 本地用户的服务类型不匹配

1. 故障描述

管理员采用本地认证方式登录设备失败。如果设备上同时打开了 Local-Server 的事件调试信息开关（通过执行 **debugging local-server event** 命令），系统会打印如下形式的调试信息：

```
*Aug  7 17:18:07:098 2021 Sysname LOCALSER/7/EVENT: -MDC=1;  Authentication failed,
unexpected user service type 64 (expected = 3072).
```

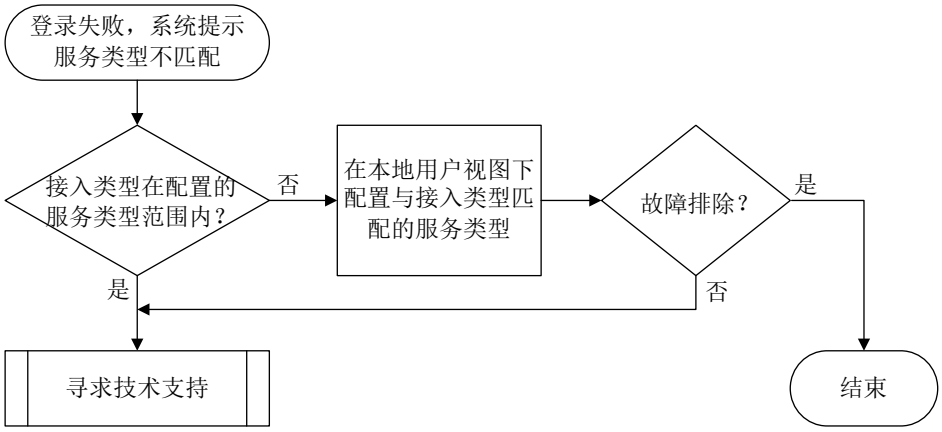
2. 常见原因

本类故障的主要原因为，用户的接入类型与设备上配置的本地用户服务类型不匹配，即用户的接入类型不在配置的服务类型范围之内。

3. 故障分析

本类故障的诊断流程如图 103 所示。

图103 本地用户服务类型不匹配的故障诊断流程图



4. 处理步骤

(1) 检查用户接入类型是否在本地用户配置的服务类型范围之内。

a. 执行 **display local-user** 命令查看本地用户的配置信息，用户服务类型由“Service type:”字段标识。

```
<Sysname> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
  State:                        Active
  Service type:                 Telnet
  User group:                   system
  Bind attributes:
  Authorization attributes:
    Work directory:             flash:
    User role list:
...
```

b. 在该用户的本地用户视图下，通过执行 **service-type** *type* 命令修改用户的服务类型为实际使用的接入类型（下例中为 SSH）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] service-type ssh
```

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、调试信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.7 登录失败固定次数后，被禁止在指定的时间内再次登录

1. 故障描述

管理员登录设备失败指定的次数后，在一定时间内被禁止再次登录设备。

2. 常见原因

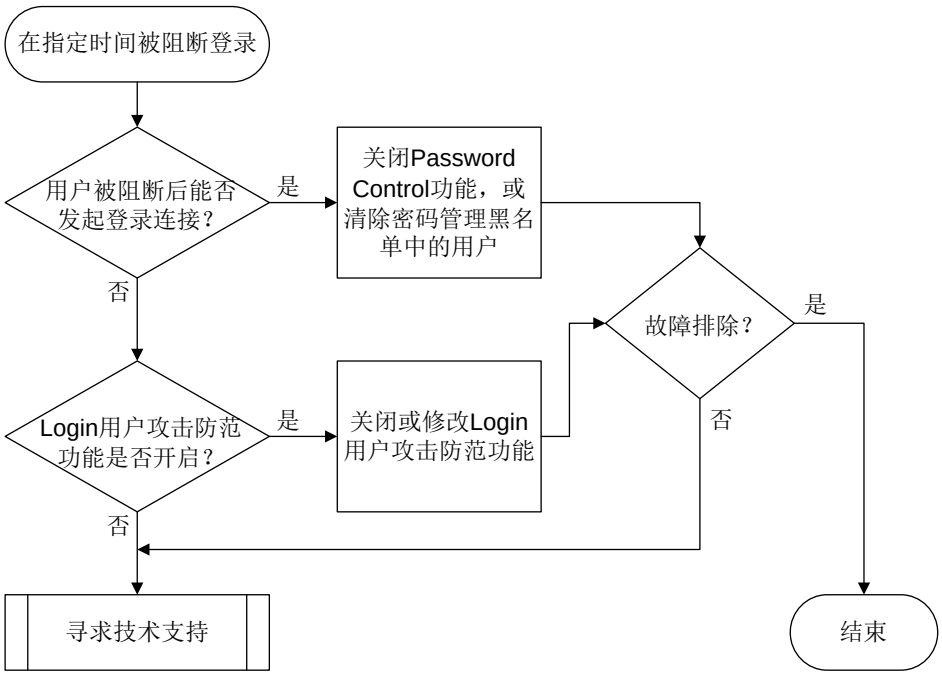
本类故障的常见原因主要包括：

- 设备上开启了 Login 用户攻击防范功能。开启该功能后，会导致 Login 用户登录失败指定的次数后，若用户的 IP 地址被加入黑名单，则设备将会丢弃来自该 IP 地址的报文，使得该用户不能在指定的阻断时长内进行登录操作。
- 用户采用本地认证方式登录设备，且设备上开启了 Password Control 功能。用户登录认证失败后，系统会将该用户加入密码管理的黑名单，并根据配置的处理措施对其之后的登录行为进行相应的限制。当用户登录失败次数超过指定值后，系统禁止该用户登录，经过一段时间后，再允许该用户重新登录。

3. 故障分析

本类故障的诊断流程如图 104 所示。

图104 指定时间内被阻断登录的故障诊断流程图



4. 处理步骤

(1) 等待一定时间后，尝试重新登录。

如果因为偶尔密码输入有误导致的禁止登录，属于正常现象，建议等待一定的时间后再次尝试重新登录。如果再次使用正确的用户名和密码登录设备遇到同样的问题，请更换其它可登录设备的管理员账号继续下面的处理步骤。

(2) 确认用户被阻断后能否发起登录连接。

- 如果该用户被阻断后，仍然可以向设备发起登录连接，但无法认证成功，则在任意视图下执行 **display password-control blacklist** 命令查看该用户是否被加入了黑名单。如果该用户在黑名单中，且显示信息中的 Lock flag 为 lock，则表示用户被锁定了。

```
<Sysname> display password-control blacklist
 Per-user blacklist limit: 100.
 Blacklist items matched: 1.
 Username                IP address           Login failures   Lock flag
 test                     3.3.3.3              4                   lock
```

对于加入黑名单的用户，有两种处理方式：

  - 在系统视图下执行 **undo password-control enable** 命令关闭全局密码管理功能。

```
<Sysname> system-view
[Sysname] undo password-control enable
```

  - 在用户视图下执行 **reset password-control blacklist** 命令清除密码管理黑名单中的用户（下例中为用户 test）。

```
<Sysname> reset password-control blacklist user-name test
```

- 如果该用户被阻断后，根本无法向设备发起登录连接，则执行步骤（3）。

(3) 检查是否开启了 Login 用户攻击防范功能。

如果当前配置中存在 **attack-defense login** 开头的相关命令，则可以根据需要关闭 Login 用户攻击防范功能，或者改变 Login 用户登录连续失败的最大次数以及登录失败后的阻断时长。

- 通过执行 **undo attack-defense login enable** 命令关闭 Login 用户攻击防范功能，并通过执行 **undo blacklist global enable** 命令关闭与之配合的全局黑名单过滤功能。

```
<Sysname> system-view
[Sysname] undo attack-defense login enable
[Sysname] undo blacklist global enable
```

- 通过执行 **attack-defense login max-attempt** 命令增加连续登录失败的最大次数，增大用户登录的尝试机会（下例为 5 次）。

```
<Sysname> system-view
[Sysname] attack-defense login max-attempt 5
```

- 通过执行 **attack-defense login block-timeout** 命令减小阻断时长（下例为 1 分钟），让用户尽快重新登录。

```
<Sysname> system-view
[Sysname] attack-defense login block-timeout 1
```

执行以上操作可能会减弱设备防范 Login 用户 DoS 攻击的力度，请慎重执行。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.8 登录失败后需要等待一定时长再进行重认证

1. 故障描述

管理员登录设备失败后，控制台无响应一定的时间，期间用户无法执行任何操作。

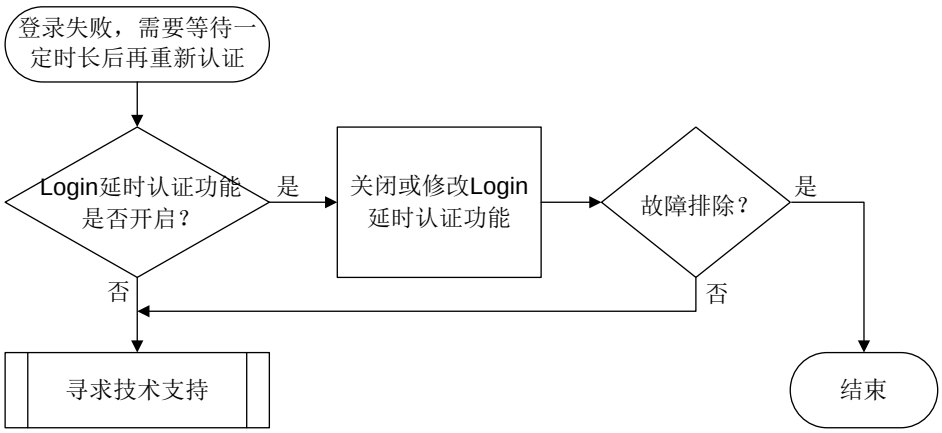
2. 常见原因

本类故障的主要原因主要为，设备上配置了 Login 延时认证功能。开启本功能后，用户登录失败后，系统将会延迟一定的时长之后再允许用户进行认证。

3. 故障分析

本类故障的诊断流程如图图 105 所示。

图105 登录失败后等待重认证的故障诊断流程图



4. 处理步骤

(1) 检查是否开启了 Login 延时认证功能。

如果当前配置中存在 **attack-defense login reauthentication-delay** 命令，则可以根据需要关闭 Login 延时认证功能，或修改重认证等待时长。

- 通过执行 **undo attack-defense login reauthentication-delay** 命令关闭延时认证功能。

```
<Sysname> system-view
[Sysname] undo attack-defense login reauthentication-delay
```

- 通过执行 **attack-defense login reauthentication-delay** *seconds* 命令减小用户登录失败后重新进行认证的等待时长（下例中为 10 秒）。

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 10
```

执行以上操作可能会减弱设备防范 Login 用户字典序攻击的力度，请慎重执行。

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.9 使用相同用户名接入设备的用户数达到上限

1. 故障描述

使用同一用户名接入设备的本地认证用户达到一定数量后，后续使用该用户名登录设备失败。

如果设备上同时打开了 Local-Server 的事件调试信息开关（通过执行 **debugging local-server event** 命令），系统会打印如下形式的调试信息：

```
*Aug 18 10:52:56:664 2021 Sysname LOCALSER/7/EVENT: -MDC=1;
 Authentication failed, the maximum number of concurrent logins already reached for the local user.
```

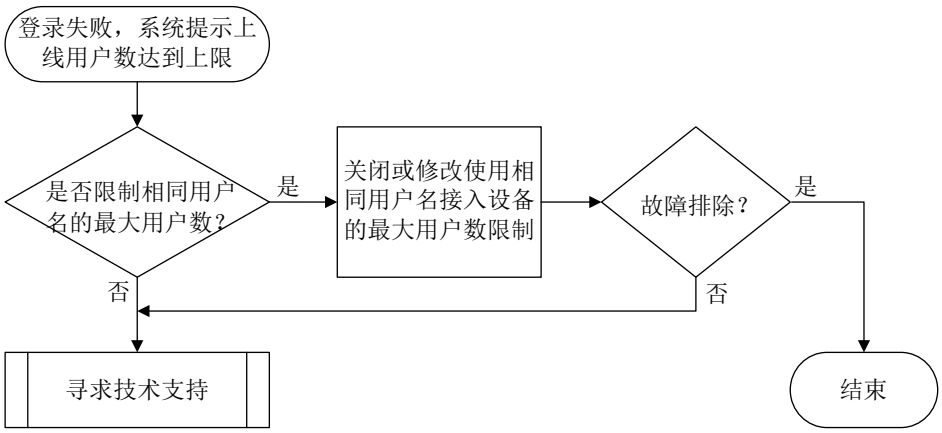
2. 常见原因

本类故障的主要原因为，设备上设置了使用当前本地用户名接入设备的最大用户数。

3. 故障分析

本类故障的诊断流程如图 106 所示。

图106 使用相同用户名的上线用户数达上限后的故障诊断流程图



4. 处理步骤

(1) 检查是否设置了使用当前本地用户名接入设备的最大用户数。

执行**display local-user** 命令，查看该用户名的本地用户配置信息。如果其中的“Access limit:”字段取值为 Enabled，则表示设置了使用当前本地用户名接入设备的最大用户数（下例中为 2）。

```
<Sysname> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
  Service type:              SSH/Telnet
  Access limit:              Enabled           Max access number: 2
  Service type:              Telnet
```

```
  User group:                 system
  Bind attributes:
  Authorization attributes:
    Work directory:           flash:
    User role list:           test
...
```

可以根据需要在本地用户视图下取消或者改变使用当前本地用户名接入设备的最大用户数。

- 通过执行 **undo access-limit** 命令取消使用当前本地用户名接入的用户数限制。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] undo access-limit
```

- 通过执行 **access-limit** *max-user-number* 命令增加最大用户数（下例中为 10）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] access-limit 10
```

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.10 相同接入类型的在线用户数达到上限

1. 故障描述

使用同一登录方式接入设备的用户达到一定数量后，后续该类用户登录设备失败。

如果设备上同时打开了相关接入模块的事件调试信息开关，系统会打印如下形式的调试信息：

```
%Aug 18 10:57:52:596 2021 Sysname TELNETD/6/TELNETD_REACH_SESSION_LIMIT: -MDC=1; Telnet client 1.1.1.1 failed to log in. The current number of Telnet sessions is 5. The maximum number allowed is (5).
```

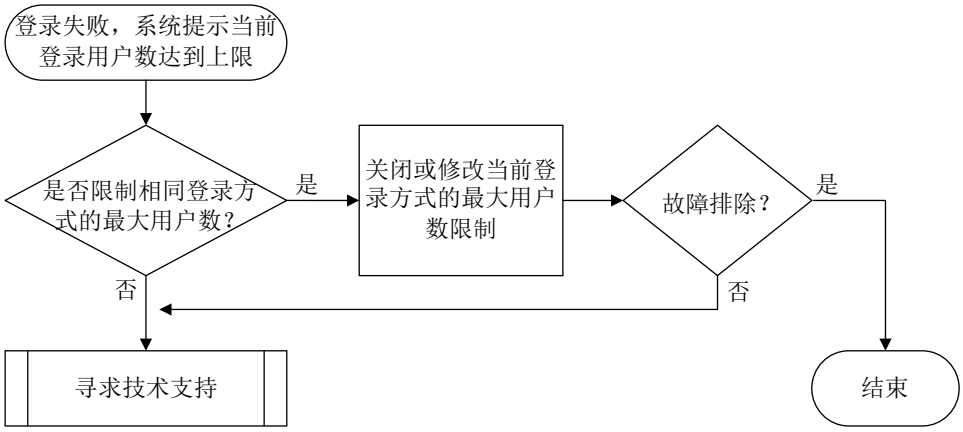
2. 常见原因

本类故障的主要常见原因为，设备上设置了采用指定登录方式登录设备并同时在线的用户数。

3. 故障分析

本类故障的诊断流程如图 107所示：

图107 使用相同登录方式接入用户数达到上限后的故障诊断流程图



4. 处理步骤

(1) 检查是否设置了采用指定登录方式登录设备并同时在线的用户数。

如果当前配置中存在 **aaa session-limit** 命令，则可以根据需要在系统视图下通过 **aaa session-limit { ftp | http | https | ssh | telnet }** *max-sessions* 命令改变使用当前登录方式接入设备的最大用户数（下例中为 32）。

```
<Sysname> system-view
[Sysname] aaa session-limit telnet 32
```

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.11 RADIUS 服务器无响应

1. 故障描述

因为服务器无响应导致使用 RADIUS 认证服务器认证/授权/计费失败。如果设备上同时打开了 RADIUS 的事件调试信息开关（通过执行 **debugging radius event** 命令），系统会打印如下形式的调试信息：

```
*Aug  8 17:49:06:143 2021 Sysname RADIUS/7/EVENT: -MDC=1; Reached the maximum retries
```

2. 常见原因

本类故障的常见原因主要包括：

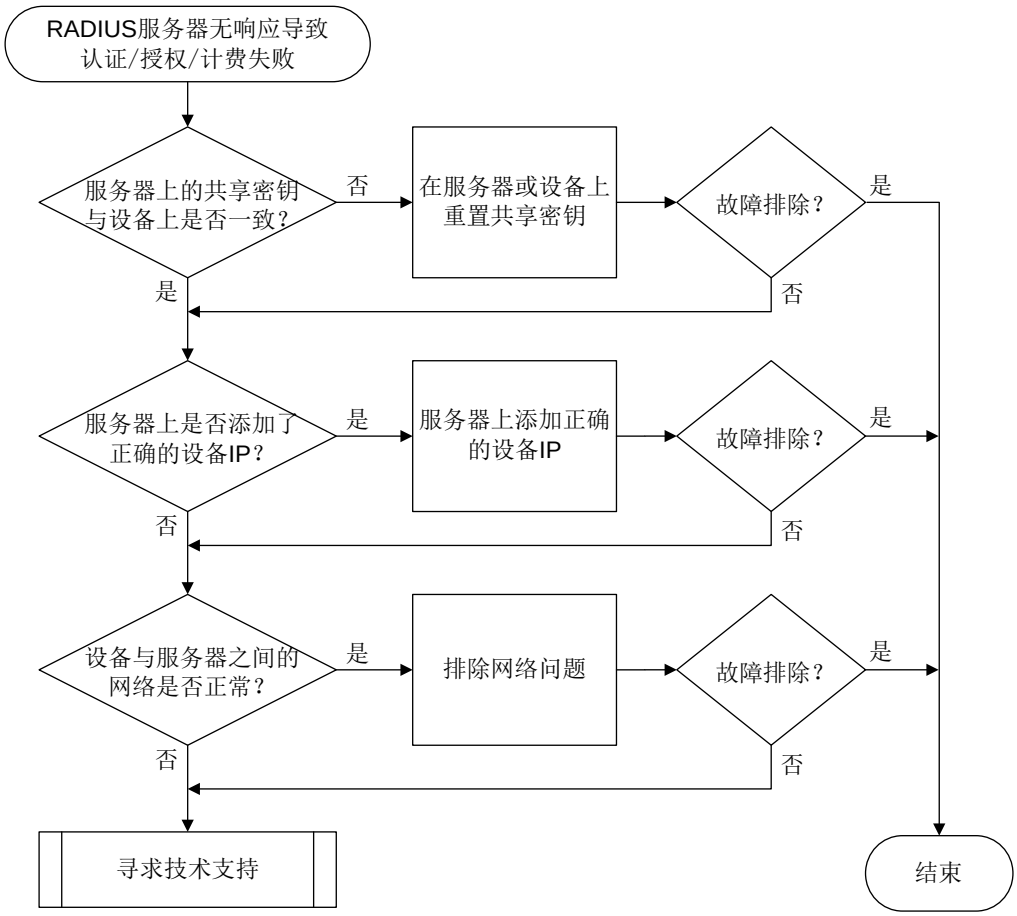
- RADIUS 服务器上配置的共享密钥与接入设备上配置的共享密钥不一致。
- RADIUS 服务器上没有添加接入设备的 IP 地址或者添加的 IP 地址不正确。

- RADIUS 服务器与接入设备之间的网络存在问题，例如中间网络存在防火墙时，防火墙阻止了 RADIUS 服务器提供 AAA 服务的端口号（缺省认证端口号：1812，缺省计费端口号：1813）。

3. 故障分析

本类故障的诊断流程如图 108 所示。

图108 RADIUS 服务器无响应的故障诊断流程图



4. 处理步骤

(1) 检查 RADIUS 服务器上配置的共享密钥与接入设备上配置的是否一致。

- 如果共享密钥配置不一致，则：
  - 在接入设备上，需要在 RADIUS 方案视图下执行 **key authentication**、**key accounting** 命令分别重新配置认证、计费共享密钥（下例中认证密钥为 123、计费密钥为 456）。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication simple 123
[Sysname-radius-radius1] key accounting simple 456
```

  - 在 RADIUS 服务器上，重新配置与接入设备交互 RADIUS 报文的共享密钥，保证与接入设备上配置的一致。
- 如果共享密钥配置一致，则执行步骤（2）。

(2) 检查 RADIUS 服务器上是否添加了接入设备的 IP 地址或者添加的 IP 地址是否正确。

RADIUS 服务器上添加的设备 IP 地址必须是接入设备发送 RADIUS 报文的源 IP 地址。接入设备发送 RADIUS 报文使用的源 IP 地址可以通过相关命令设置。

接入设备按照以下顺序选择发送 RADIUS 报文使用的源 IP 地址：

a. RADIUS 方案视图下配置的 NAS-IP 地址（通过 **nas-ip** 命令）。

b. 系统视图下的配置的源 NAS-IP 地址（通过 **radius nas-ip** 命令）。

c. 发送 RADIUS 报文的出接口的 IP 地址。

(3) 检查设备和服务器之间的网络是否存在问题。

首先使用 ping 等手段排除设备与服务器之间的网络可达性，然后排查该网络中是否存在防火墙等设备。通常，如果网络中存在防火墙设备且不允许目的 UDP 端口号为 RADIUS 服务器端口号的报文通过（缺省的 RADIUS 认证端口号为 1812，缺省的 RADIUS 计费端口号为 1813），RADIUS 报文将被丢弃。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、调试信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.12 HWTACACS 服务器无响应

1. 故障描述

使用 HWTACACS 认证服务器认证/授权/计费失败。如果同时在设备上执行 **debugging hwtacacs event** 命令打开 HWTACACS 事件调试信息开关，系统打印的事件调试信息中将出现“Connection timed out.”。

2. 常见原因

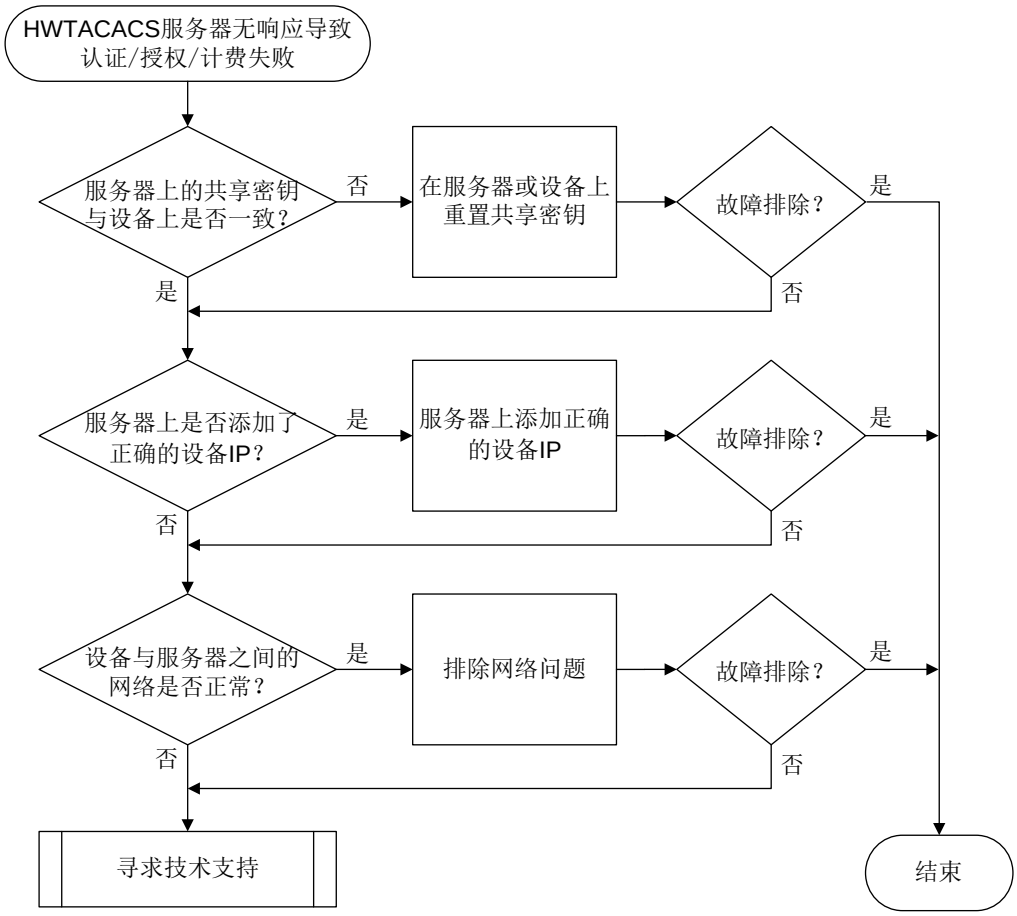
本类故障的常见原因主要包括：

- HWTACACS 服务器上配置的共享密钥与接入设备上配置的共享密钥不一致。
- HWTACACS 服务器上没有添加接入设备的 IP 地址或者添加的 IP 地址不正确。
- HWTACACS 服务器与接入设备之间的网络存在问题，例如中间网络存在防火墙时，防火墙阻止了 HWTACACS 服务器提供 AAA 服务的端口号（缺省认证/授权/计费端口号为 49）。

3. 故障分析

本类故障的诊断流程如图 109 所示。

图109 HWTACACS 服务器无响应的故障诊断流程图



4. 处理步骤

(1) 检查 HWTACACS 服务器上配置的共享密钥与接入设备上配置的是否一致。

- 如果共享密钥配置不一致，则：
  - 在接入设备上，需要在 HWTACACS 方案视图下执行 **key authentication**、**key authorization**、**key accounting** 命令重新配置认证、授权、计费共享密钥（下例中认证和授权密钥为 123、计费密钥为 456）。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key authentication simple 123
[Sysname-hwtacacs-hwt1] key authorization simple 123
[Sysname-hwtacacs-hwt1] key accounting simple 456
```

  - 在 HWTACACS 服务器上，重新配置与接入设备交互 HWTACACS 报文的共享密钥，保证与接入设备上配置的一致。
- 如果共享密钥配置一致，则执行步骤（2）。

(2) 检查 HWTACACS 服务器上是否添加了接入设备的 IP 地址或者添加的 IP 地址是否正确。

HWTACACS 服务器上添加的设备 IP 地址必须是接入设备发送 HWTACACS 报文的源 IP 地址。接入设备发送 HWTACACS 报文使用的源 IP 地址可以通过相关命令设置。

接入设备按照以下顺序选择发送 HWTACACS 报文使用的源 IP 地址：

a. HWTACACS 方案视图下配置的源 IP 地址（通过 **nas-ip** 命令）。

b. 系统视图下的配置的源 IP 地址（通过 **hwtacacs nas-ip** 命令）。

c. 发送 HWTACACS 报文的出接口的 IP 地址。

(3) 检查设备和服务器之间的网络是否存在问题。

首先使用 ping 等手段排除设备与服务器之间的网络可达性，然后排查该网络中是否存在防火墙等设备。通常，如果网络中存在防火墙设备且不允许目的 TCP 端口号为 HWTACACS 服务器端口号的报文通过（缺省的 HWTACACS 认证/授权/计费端口号为 49），HWTACACS 报文将被丢弃。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、调试信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.13 用户接入类型与 RADIUS 服务器下发的 Login-Service 属性值不匹配

1. 故障描述

由于设备不支持 RADIUS 服务器下发的 Login-Service 属性值，导致用户认证失败。

打开设备上 RADIUS 的报文调试信息开关（通过执行 **debugging radius packet** 命令），在如下形式的调试信息中查看到服务器下发的 Login-Service 属性类型为设备不支持的类型：

```
*Aug  3 02:33:18:707 2021 Sysname RADIUS/7/PACKET:
    Service-Type=Framed-User
    Idle-Timeout=66666
    Session-Timeout=6000
    Login-Service=TCP-Clear
```

2. 常见原因

本类故障的主要原因为，用户登录的业务类型与服务器下发的 Login-Service 属性所指定的业务类型不一致。

Login-Service 属性由 RADIUS 服务器下发给用户，标识认证用户的业务类型。当前设备支持的 Login-Service 属性取值如下：

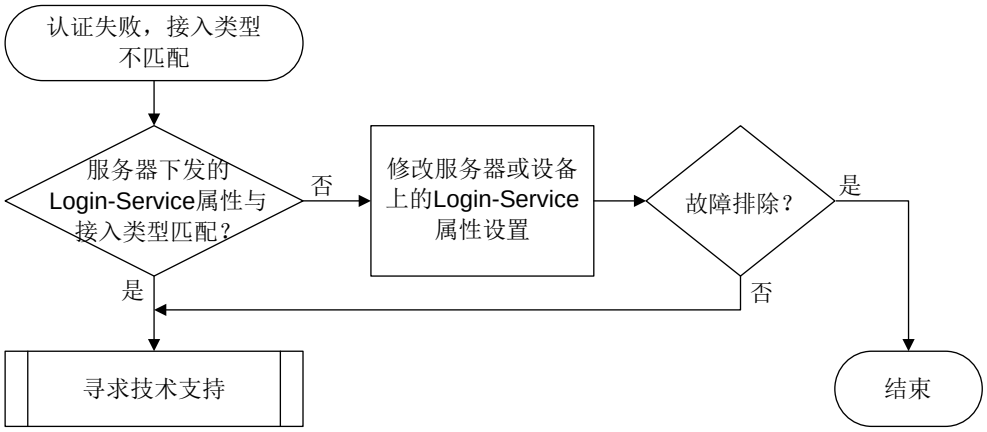
- 0：Telnet（标准属性）
- 50：SSH（扩展属性）
- 51：FTP（扩展属性）
- 52：Terminal（扩展属性）
- 53：HTTP（扩展属性）
- 54：HTTPS（扩展属性）

可以通过命令行设置设备对 Login-Service 属性的检查方式，控制设备对用户进行业务类型一致性检查的方式。

3. 故障分析

本类故障的诊断流程如图 110 所示。

图110 用户接入类型与 RADIUS 服务器下发的 Login-Service 属性值不匹配的故障诊断流程图



4. 处理步骤

(1) 检查 RADIUS 服务器下发的 Login-Service 属性与接入类型是否匹配。

在接入设备上执行 **display radius scheme** 命令，查看 RADIUS 方案下的“Attribute 15 check-mode”字段取值：

- 取值为 Loose，表示采用松散检查方式，即使用 Login-Service 的标准属性值对用户业务类型进行检查。对于 SSH、FTP、Terminal 用户，在 RADIUS 服务器下发的 Login-Service 属性值为 0（表示用户业务类型为 Telnet）时才，这类用户才能够通过认证。
- 取值为 Strict，表示采用严格检查方式，即使用 Login-Service 的标准属性值以及扩展属性值对用户业务类型进行检查。对于 SSH、FTP、Terminal 用户，当 RADIUS 服务器下发的 Login-Service 属性值为对应的扩展取值时，这类用户才能够通过认。

如果 RADIUS 服务器下发给用户的 Login-Service 属性不属于设备支持的 Login-Service 属性范围，则可以选用如下方法之一解决：

- 在 RADIUS 服务器上，设置服务器不下发 Login-Service 属性或者修改下发的属性值为接入设备支持的取值。
- 在接入设备上，进入相应的 RADIUS 方案，通过执行 **attribute 15 check-mode** 命令修改对 Login-Service 属性的检查方式（下例中为松散检查方式）。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 15 check-mode loose
```

(2) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、调试信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

16.2.14 本地认证登录失败

1. 故障描述

管理员采用本地认证登录设备失败。

2. 常见原因

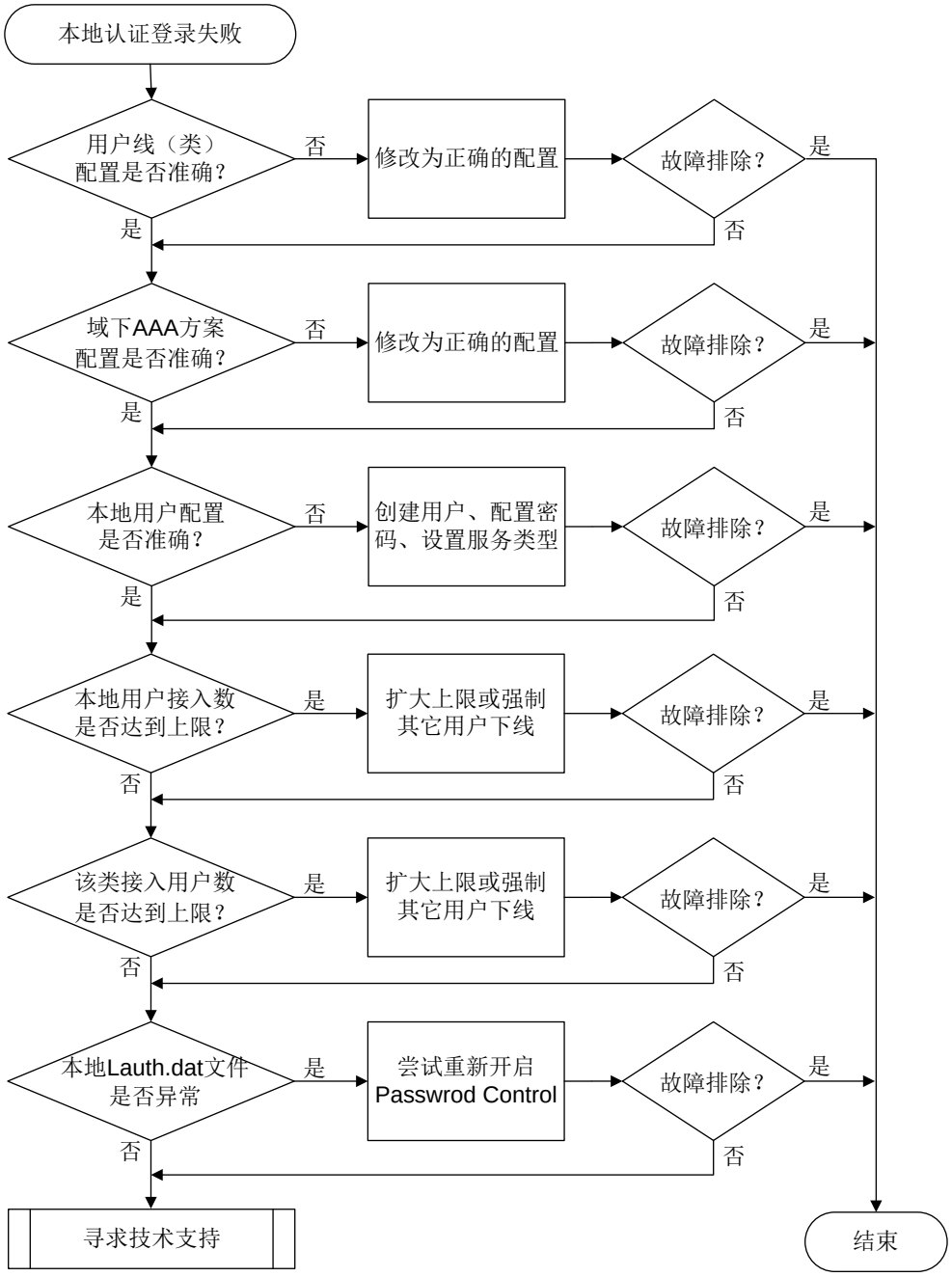
本类故障的常见原因主要包括：

- 用户线下的认证方式配置错误。
- VTY 用户线下支持的协议类型不正确。
- ISP 域下配置的认证、授权、计费方案错误。
- 本地用户不存在、用户密码错误，或服务类型错误。
- 本地用户接入数量达到上限。
- 登录设备的用户数量到达上限。
- 全局密码管理功能开启的情况下，设备本地的 lauth.dat 文件异常。

3. 故障分析

本类故障的诊断流程如图 111 所示。

图111 本地认证登录失败的故障诊断流程图



4. 处理步骤

说明

Web、NETCONF over SOAP、FTP 类登录故障无需关心用户线（类）下的配置，其它排障步骤相同。

(1) 检查用户线下的配置。

执行 **line vty** *first-number* [*last-number*]命令进入指定的 VTY 用户线视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

(2) 检查用户线类下的配置。

用户线视图下的配置优先于用户线类视图下的配置。若用户线视图下未配置，则需要继续检查用户线类视图下的配置。

执行 **line class vty** 命令进入 VTY 用户线类视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

如果用户线和用户线类下的配置均不准确，请按照需要在指定的用户线或用户线类下设置认证方案为 **scheme**，并设置用户登录支持的协议类型。

(3) 检查 ISP 域下的认证、授权、计费方案配置是否准确。

执行 **display domain** 命令，查看显示信息：

- 如果用户的登录用户名中携带了域名（假设为 test），则查看该域下的“Login authentication scheme:”字段取值是否为 Local。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为 Local。

```
<Sysname> display domain test

Domain: test
  State: Active
  Login   authentication scheme:  Local
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  NAS-ID: N/A
  DHCPv6-follow-IPv6CP timeout: 60 seconds
  Authorization attributes:
    Idle cut: Disabled
    Session timeout: Disabled
    IGMP access limit: 4
    MLD access limit: 4
```

- 如果用户的登录用户名中未携带域名，则在系统视图下执行 **display this** 命令查看是否存在 **domain default enable** *isp-name* 配置。（下例中缺省域名为 system）。

```
#
domain default enable system
```

#

– 如果存在该配置，则执行 **display domain** 命令查看 *isp-name* 域下的“Login authentication scheme:”字段取值是否为“Local”。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“Local”。
– 如果不存在该配置，则执行 **display domain** 命令查看 system 域下的“Login authentication scheme:”字段取值是否为“Local”。如果 system 域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“Local”。

授权、计费配置确认方式与认证类似，不再赘述。如果以上配置不准确，请在相关 ISP 下配置 Login 用户的认证/授权/计费方案均为 Local。

(4) 检查用户名和密码是否正确。

执行 **display local-user** 命令查看是否存在对应的本地用户配置。

- 如果本地用户存在，则执行 **local-user** *username* **class manage** 命令进入本地用户视图，然后通过 **display this** 命令查看该视图下是否配置了密码，以及 **service-type** 配置是否为所需的服务类型。
  – 若需要用户密码，则尝试重置一次密码（下例中为 123456TESTplat&!）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password simple 123456TESTplat&!
```

  – 若服务类型错误，则配置与登录方式匹配的服务类型（下例中为 SSH）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] service-type ssh
```

- 如果本地用户不存在，则执行 **local-user** *username* **class manage** 命令创建一个设备管理类本地用户（下例中用户名为 test），并按需配置密码和服务类型。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test]
```

(5) 检查使用该本地用户名接入的用户数是否达到上限。

在本地用户视图下执行 **display this** 命令查看是否存在 **access-limit** 配置。

- 如果 **access-limit** 配置存在，则执行 **display local-user** *username* **class manage** 命令查看“Current access number:”字段取值是否达到配置的上限值。如果达到上限值，则根据需要采取以下措施之一：
  – 在该本地用户视图下执行 **access-limit** 命令扩大用户数上限（下例中为 20）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] access-limit 20
```

  – 在用户视图下执行 **free** 命令强制其它在线用户下线（下例中为强制释放 VTY1 上建立的所有连接）。

```
<Sysname> free line vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

- 如果 **access-limit** 配置不存在，或者用户数未达到上限值，则继续定位。

(6) 检查指定登录类型的在线用户数是否到达上限。

a. 在系统视图下执行 **display this** 命令查看是否存在 **aaa session-limit** 的配置，若无此配置，则说明采用了缺省值 32。

```
#
 aaa session-limit ftp 33
 domain default enable system
#
```

b. 执行 **display users** 查看当前用户线的用户登录情况，确认是否已到用户数上限。

c. 如果在线用户数到达上限，则根据需要采取以下措施之一：

- 在系统视图下执行 **aaa session-limit** 命令扩大用户数上限。
- 在用户视图下执行 **free** 命令强制其它在线用户下线。

(7) 检查本地 lauth.dat 文件是否正常。

开启全局密码管理功能后，设备会自动生成 lauth.dat 文件记录本地用户的认证、登录信息。如果手工删除或修改该文件，会造成本地认证异常。因此，请首先执行 **display password-control** 命令查看设备上是否开启了全局密码管理功能。

- 如果该文件不存在、大小为 0 或者很小（若小于 20B，则大概率发生了异常），请优先联系技术支持人员协助处理，若当前配置需求紧迫，可尝试重新开启全局密码管理功能来解决此问题。

```
<Sysname> dir
Directory of flash: (EXT4)
   0 drw-           - Aug 16 2021 11:45:37   core
   1 drw-           - Aug 16 2021 11:45:42   diagfile
   2 drw-           - Aug 16 2021 11:45:57   dlp
   3 -rw-         713 Aug 16 2021 11:49:41   ifindex.dat
   4 -rw-          12  Sep 01 2021 02:40:01   lauth.dat
...
<Sysname> system-view
[Sysname] undo password-control enable
[Sysname] password-control enable
```

- 若未开启，则忽略此步骤。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、诊断信息。
- 打开 Local-Server **调试信息开关（通过 debugging local-server all** 命令），收集设备的调试信息。

5. 告警与日志

相关告警

模块名：HH3C-UI-MAN-MIB

- hh3cLogInAuthenFailure (1.3.6.1.4.1.25506.2.2.1.1.3.0.3)

模块名：HH3C-SSH-MIB

- hh3cSSHUserAuthFailure (1.3.6.1.4.1.25506.2.22.1.3.0.1)

相关日志

- LOGIN/5/LOGIN_FAILED
- SSHS/6/SSHS_AUTH_FAIL

16.2.15 RADIUS 认证登录失败

1. 故障描述

管理员采用 RADIUS 认证登录设备失败。

2. 常见原因

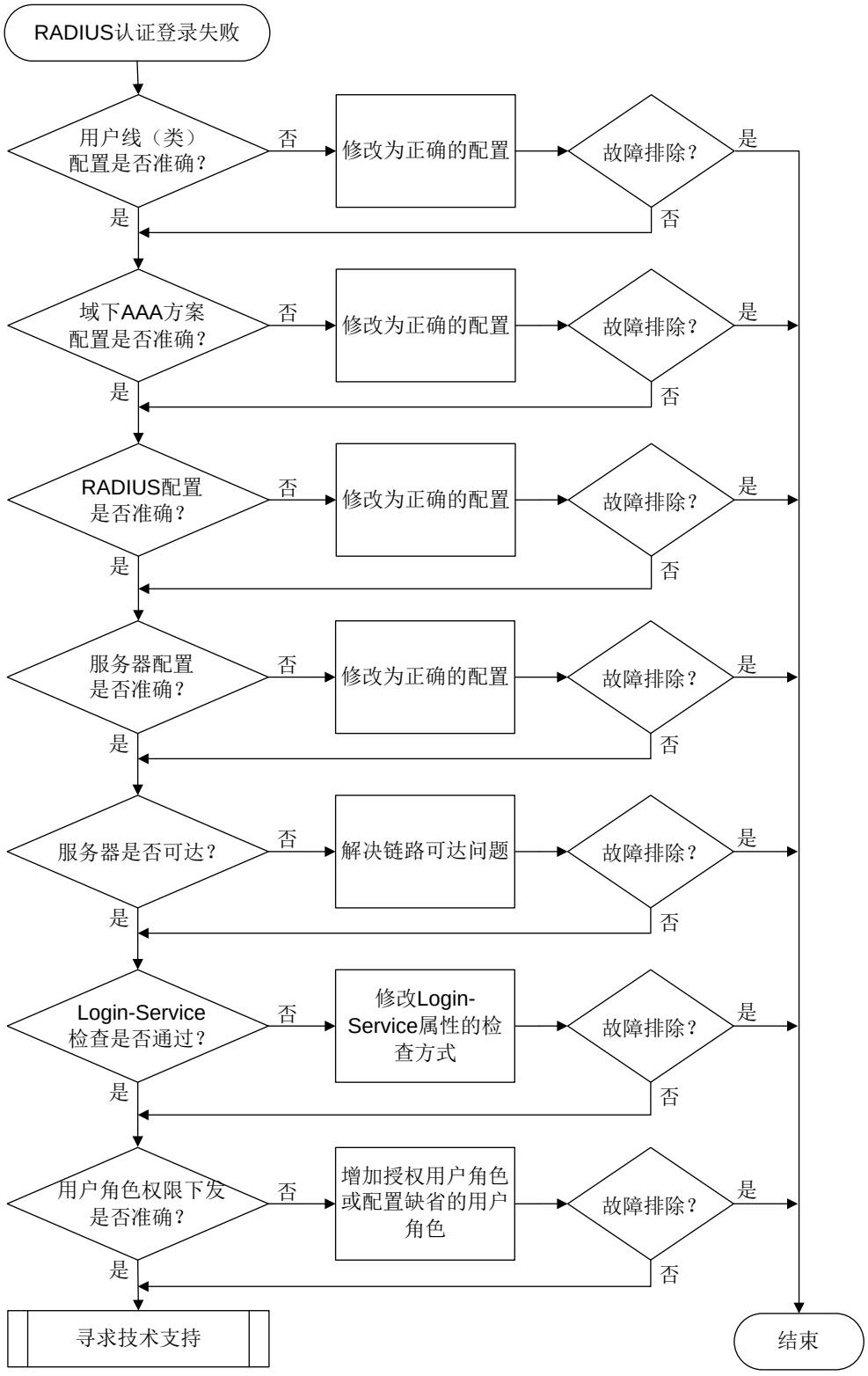
本类故障的常见原因主要包括：

- 用户线下的认证方式配置错误。
- VTY 用户线下支持的协议类型不正确。
- ISP 域下配置的认证、授权、计费方案错误。
- 与 RADIUS 服务器交互失败。
- RADIUS 服务器下发的 Login-Service 属性值不正确。
- RADIUS 服务器未下发用户角色权限。

3. 故障分析

本类故障的诊断流程如图 112所示。

图112 RADIUS 认证登录失败的故障诊断流程图



4. 处理步骤

说明

Web、NETCONF over SOAP、FTP 类登录故障无需关心用户线（类）下的配置，其它排障步骤相同。

(1) 检查用户线下的配置。

执行 **line vty** *first-number* [*last-number*]命令进入指定的 VTY 用户线视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

(2) 检查用户线类下的配置。

用户线视图下的配置优先于用户线类视图下的配置。若用户线视图下未配置，则需要继续检查用户线类视图下的配置。

执行 **line class vty** 命令进入 VTY 用户线类视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

如果用户线和用户线类下的配置均不准确，请按照需要，在指定的用户线或用户线类下设置认证方案为 **scheme**，并设置用户登录支持的协议类型。

(3) 检查 ISP 域下的认证、授权、计费方案配置是否准确。

执行 **display domain** 命令，查看显示信息：

- 如果用户的登录用户名中携带了域名（假设为 test），则查看该域下的“Login authentication scheme:”字段取值是否为“RADIUS=*xx*”。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“RADIUS=*xx*”。

```
<Sysname> display domain test

Domain: test
  State: Active
  Login   authentication scheme:  RADIUS=rds
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  NAS-ID: N/A
  DHCPv6-follow-IPv6CP timeout: 60 seconds
```

```
  Authorization attributes:
    Idle cut: Disabled
    Session timeout: Disabled
    IGMP access limit: 4
    MLD access limit: 4
```

- 如果用户的登录用户名中未携带域名，则在系统视图下执行 **display this** 命令查看是否存在 **domain default enable** *isp-name* 配置（下例中缺省域名为 system）。

```
#
domain default enable system
#
```

  - 如果存在该配置，则执行 **display domain** 命令查看 *isp-name* 域下的“Login authentication scheme:”字段取值是否为“RADIUS=*xx*”。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“RADIUS=*xx*”。
  - 如果不存在该配置，则执行 **display domain** 命令查看 system 域下的“Login authentication scheme:”字段取值是否为“RADIUS=*xx*”。如果 system 域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“RADIUS=*xx*”。

授权、计费配置确认方式与认证类似，不再赘述。如果以上配置不准确，请在相关 ISP 域下配置 Login 用户采用 RADIUS 认证/授权/计费方案（下例中认证/授权/计费均采用 RADIUS 方案 rd1）。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd1
[Sysname-isp-test] authorization login radius-scheme rd1
[Sysname-isp-test] accounting login radius-scheme rd1
```

(4) 通过 RADIUS 的调试信息辅助排查如下故障。

- 执行 **debugging radius packet** 命令打开 RADIUS 报文调试信息开关，如果系统打印 Authentication reject 类的报文调试信息，则表示用户的认证请求被服务器拒绝。因此，需要继续查看 RADIUS 服务器上记录的认证日志，并通过日志中描述的失败原因联系服务器管理员进行相应的处理。
- 执行 **debugging radius error** 命令打开 RADIUS 错误调试信息开关，如果系统打印错误调试信息“Invalid packet authenticator.”，则表示设备与服务器的共享密钥不匹配，可以尝试在 RADIUS 方案下设置与服务器匹配的共享密钥。
- 执行 **debugging radius event** 命令打开 RADIUS 事件调试信息开关，如果系统打印事件调试信息“Response timed out. ”，则表示设备与服务器之间不可达，可以尝试排查设备和服务器中间链路不通的问题。

(5) 检查 RADIUS 服务器下发的 Login-Service 属性值是否为设备支持的业务类型。

执行 **debugging radius packet** 命令打开 RADIUS 的报文调试信息开关后，查看 RADIUS 服务器下发的 Login-Service 属性情况，并采用“16.2.13 用户接入类型与 RADIUS 服务器下发的 Login-Service 属性值不匹配”介绍的方法解决故障。

(6) 检查 RADIUS 服务器是否下发了正确的用户角色权限。

执行 **debugging radius all** 命令打开所有 RADIUS 调试信息开关后，如果用户输入用户名和密码后连接直接断开，且没有异常的 RADIUS 事件调试信息以及 RADIUS 错误调试信息输出，则有可能是 RADIUS 服务器未给用户下发用户角色或下发的用户角色错误导致。此时，可以查看 RADIUS 报文调试信息中是否包含“shell:roles="xx"”或“Exec-Privilege=xx”字段。

- 如果不包含，则表示 RADIUS 服务器未给用户下发用户角色权限，则可以选用如下方法之一解决：
  - 在设备侧，可以通过执行 **role default-role enable** *rolename* 命令使能缺省用户角色授权功能，使得用户在没有被服务器授权任何角色的情况下，具有一个缺省的用户角色。

    ```
    <Sysname> system-view
    [Sysname] role default-role enable
    ```

  - 联系 RADIUS 服务器管理员，为用户下发合适的用户角色。
- 如果包含，但指定的用户角色在设备上不存在，则需要联系 RADIUS 服务器管理员修改用户角色设置或者在设备上通过 **user-role** *role-name* 命令创建对应的用户角色。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、诊断信息。
- 打开 RADIUS 调试信息开关（通过 **debugging radius all** 命令），收集设备的调试信息。

5. 告警与日志

相关告警

模块名：HH3C-UI-MAN-MIB

- hh3cLogInAuthenFailure (1.3.6.1.4.1.25506.2.2.1.1.3.0.3)

模块名：HH3C-SSH-MIB

- hh3cSSHUserAuthFailure (1.3.6.1.4.1.25506.2.22.1.3.0.1)

相关日志

- LOGIN/5/LOGIN_AUTHENTICATION_FAILED
- LOGIN/5/LOGIN_FAILED
- SSHS/6/SSHS_AUTH_FAIL

16.2.16 HWTACACS 认证登录失败

1. 故障描述

管理员采用 HWTACACS 认证登录设备失败。

2. 常见原因

本类故障的常见原因主要包括：

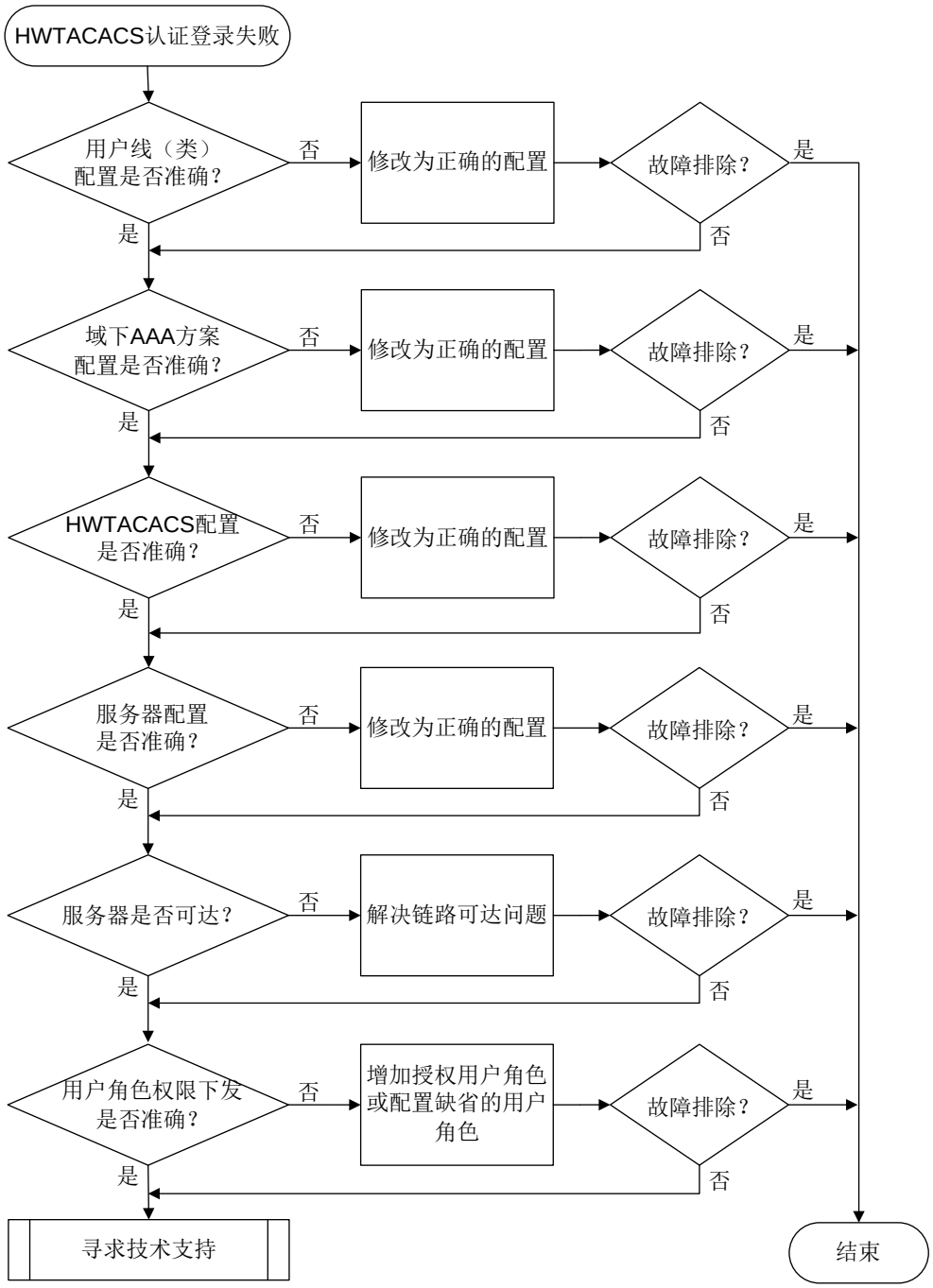
- 用户线下的认证方式配置错误。
- VTY 用户线下支持的协议类型不正确。
- ISP 域下配置的认证、授权、计费方案错误。

- 与 HWTACACS 服务器交互失败。
- HWTACACS 服务器未下发用户角色权限。

3. 故障分析

本类故障的诊断流程如图 113 所示。

图113 HWTACACS 认证登录失败的故障诊断流程图



4. 处理步骤

说明

Web、NETCONF over SOAP、FTP 类登录故障无需关心用户线（类）下的配置，其它排障步骤相同。

(1) 检查用户线下的配置。

执行 **line vty** *first-number* [*last-number*]命令进入指定的 VTY 用户线视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

(2) 检查用户线类下的配置。

用户线视图下的配置优先于用户线类视图下的配置。若用户线视图下未配置，则需要继续检查用户线类视图下的配置。

执行 **line class vty** 命令进入 VTY 用户线类视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。
- 如果用户线和用户线类下的配置均不准确，请按照需要，在指定的用户线或用户线类下设置认证方案为 **scheme**，并设置用户登录支持的协议类型。

(3) 检查 ISP 域下的认证、授权、计费方案配置是否准确。

执行 **display domain** 命令，查看显示信息：

- 如果用户的登录用户名中携带了域名（假设为 test），则查看该域下的“Login authentication scheme:”字段取值是否为“HWTACACS=*xx*”。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“HWTACACS=*xx*”。

```
<Sysname> display domain test

Domain: test
  State: Active
  Login   authentication scheme:  HWTACACS=hwt1
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  NAS-ID: N/A
```

```
  DHCPv6-follow-IPv6CP timeout: 60 seconds
  Authorization attributes:
    Idle cut: Disabled
    Session timeout: Disabled
    IGMP access limit: 4
    MLD access limit: 4
```

- 如果用户的登录用户名中未携带域名，则在系统视图下执行 **display this** 命令查看是否存在 **domain default enable** *isp-name* 配置。（下例中缺省域名为 system）。

```
#
domain default enable system
#
```

  - 如果存在该配置，则执行 **display domain** 命令查看 *isp-name* 域下的“Login authentication scheme:”字段取值是否为“HWTACACS=*xx*”。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“HWTACACS=*xx*”。
  - 如果不存在该配置，则执行 **display domain** 命令查看 system 域下的“Login authentication scheme:”字段取值是否为“HWTACACS=*xx*”。如果 system 域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“HWTACACS=*xx*”。

授权、计费配置确认方式与认证类似，不再赘述。如果以上配置不准确，请在相关 ISP 域下配置 Login 用户采用 HWTACACS 认证/授权/计费方案（下例中认证/授权/计费均采用 HWTACACS 方案 hwt1）。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login hwtacacs-scheme hwt1
[Sysname-isp-test] authorization login hwtacacs-scheme hwt1
[Sysname-isp-test] accounting login hwtacacs-scheme hwt1
```

(4) 通过 HWTACACS 的调试信息辅助排查如下故障。

- 执行 **debugging hwtacacs send-packet** 和 **debugging hwtacacs receive-packet** 命令打开 HWTACACS 报文发送/接收调试信息，如果系统打印应答报文调试信息中包含“status: STATUS_FAIL”，则表示用户的认证请求被服务器拒绝。因此，需要继续查看 HWTACACS 服务器认证日志中描述的失败原因，并根据具体的失败原因继续定位。
- 执行 **debugging hwtacacs error** 命令打开 HWTACACS 错误调试信息开关，如果系统打印错误调试信息“Failed to get available server.”，则通常表示设备与服务器的共享密钥不匹配，可以尝试在 HWTACACS 方案下设置与服务器匹配的共享密钥。
- 执行 **debugging hwtacacs event** 命令打开 HWTACACS 事件调试信息开关，如果系统打印事件调试信息“Connection timed out.”，则表示设备与服务器之间不可达，可以尝试排查设备和服务器中间链路不通的问题。

(5) 检查 HWTACACS 服务器是否下发了正确的用户角色权限。

执行 **debugging hwtacacs all** 命令打开所有 HWTACACS 调试信息开关后，如果发现客户端登录时直接断开连接，且没有异常的 HWTACACS 事件调试信息以及 HWTACACS 错误调试信息输出，则有可能是 HWTACACS 服务器未给用户下发用户角色权限导致。此时，可以查看 HWTACACS 的接收报文调试信息是否包含“priv-lvl=xx”或“roles=xx”字段。

- 如果不包含，则表示 HWTACACS 服务器未给用户下发用户角色权限，则可以选用如下方法之一解决：
  - 在设备侧，可以通过执行 **role default-role enable** *rolename* 命令使能缺省用户角色授权功能，使得用户在没有被服务器授权任何角色的情况下，具有一个缺省的用户角色。

    ```
    <Sysname> system-view
    [Sysname] role default-role enable
    ```
  - 联系 HWTACACS 服务器管理员，为用户下发合适的用户角色。HWTACACS 服务器上的授权角色配置必须满足格式：roles="*name1 name2 namen*"，其中 *name1*、*name2*、*namen* 为要授权下发给用户的用户角色，可为多个，并使用空格分隔。
- 如果包含，但指定的用户角色在设备上不存在，则需要联系 RADIUS 服务器管理员修改用户角色设置或者在设备上通过 **user-role** *role-name* 命令创建对应的用户角色。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。
- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、诊断信息。
- 打开 HWTACACS 调试信息开关（通过 **debugging hwtacacs all** 命令），收集设备的调试信息。

5. 告警与日志

相关告警

模块名：HH3C-UI-MAN-MIB

- hh3cLogInAuthenFailure (1.3.6.1.4.1.25506.2.2.1.1.3.0.3)

模块名：HH3C-SSH-MIB

- hh3cSSHUserAuthFailure (1.3.6.1.4.1.25506.2.22.1.3.0.1)

相关日志

- LOGIN/5/LOGIN_AUTHENTICATION_FAILED
- LOGIN/5/LOGIN_FAILED
- SSHS/6/SSHS_AUTH_FAIL

16.2.17 LDAP 认证登录失败

1. 故障描述

管理员采用 LDAP 认证登录设备失败。

2. 常见原因

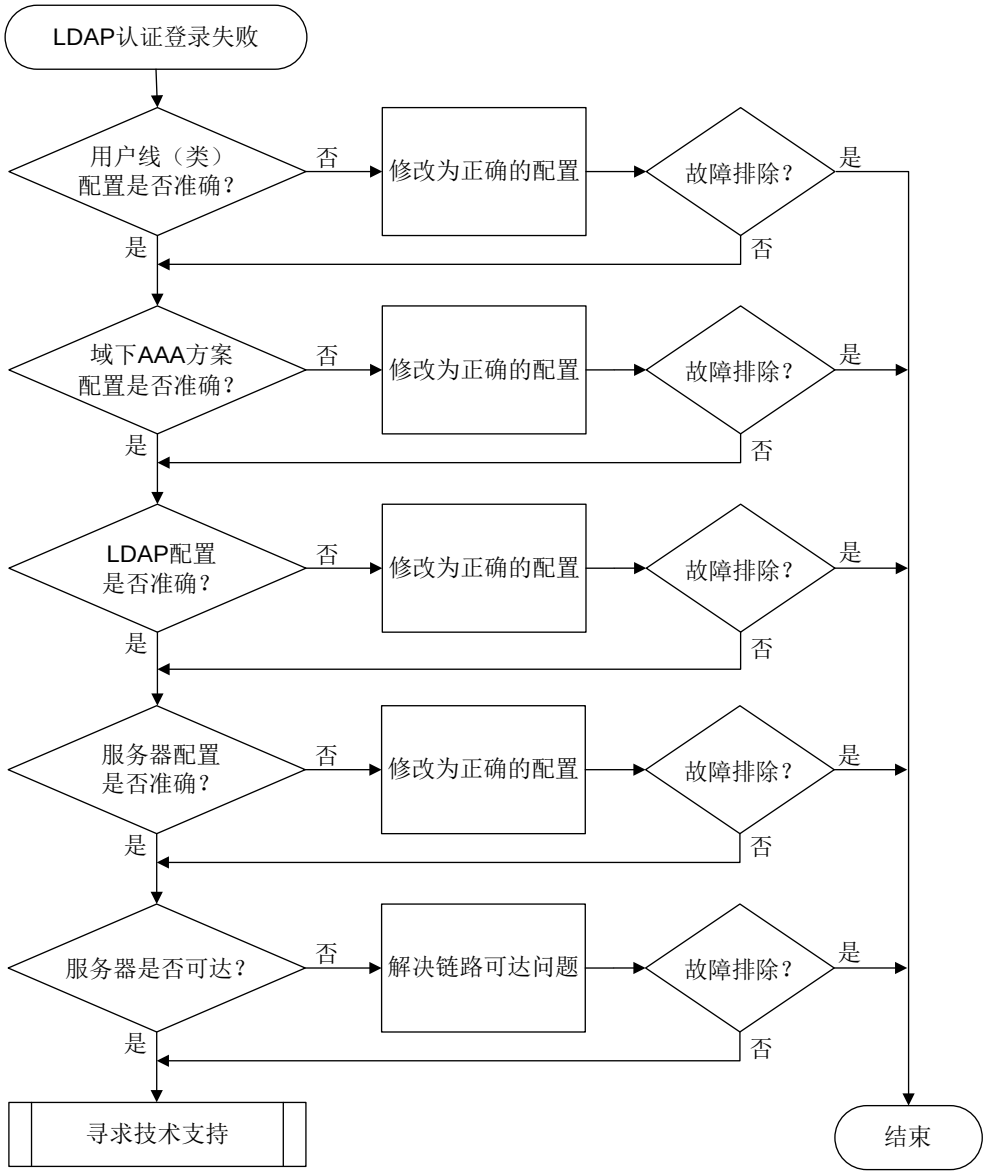
本类故障的常见原因主要包括：

- 用户线下的认证方式配置错误。
- VTY 用户线下支持的协议类型不正确。
- ISP 域下配置的认证、授权、计费方案错误。
- 与 LDAP 服务器交互失败。

3. 故障分析

本类故障的诊断流程如图 114 所示。

图114 LDAP 认证登录失败的故障诊断流程图



4. 处理步骤

说明

Web、NETCONF over SOAP、FTP 类登录故障无需关心用户线（类）下的配置，其它排障步骤相同。

(1) 检查用户线下的配置。

执行 **line vty** *first-number* [*last-number*]命令进入指定的 VTY 用户线视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

(2) 检查用户线类下的配置。

用户线视图下的配置优先于用户线类视图下的配置。若用户线视图下未配置，则需要继续检查用户线类视图下的配置。

执行 **line class vty** 命令进入 VTY 用户线类视图，并通过 **display this** 命令查看如下配置是否准确：

- **authentication-mode** 是否配置为 **scheme**。
- 对于 Telnet 登录：**protocol inbound** 是否配置为 **telnet** 或为缺省情况。
- 对于 SSH 登录：**protocol inbound** 是否配置为 **ssh** 或为缺省情况。

如果用户线和用户线类下的配置均不准确，请按照需要，在指定的用户线或用户线类下设置认证方案为 **scheme**，并设置用户登录支持的协议类型。

(3) 检查 ISP 域下的认证、授权、计费方案配置是否准确。

执行 **display domain** 命令，查看显示信息：

- 如果用户的登录用户名中携带了域名（假设为 test），则查看该域下的“Login authentication scheme:”字段取值是否为“LDAP=*xx*”。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“LDAP=*xx*”。

```
<Sysname> display domain test

Domain: test
  State: Active
  Login   authentication scheme:  LDAP=ldp
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  NAS-ID: N/A
  DHCPv6-follow-IPv6CP timeout: 60 seconds
  Authorization attributes:
    Idle cut: Disabled
    Session timeout: Disabled
    IGMP access limit: 4
    MLD access limit: 4
```

- 如果用户的登录用户名中未携带域名，则在系统视图下执行 **display this** 命令查看是否存在 **domain default enable** *isp-name* 配置（下例中缺省域名为 system）。

```
#
domain default enable system
```

#

– 如果存在该配置，则执行 **display domain** 命令查看 *isp-name* 域下的“Login authentication scheme:”字段取值是否为“LDAP=*xx*。如果该域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“LDAP=*xx*”。
– 如果不存在该配置，则执行 **display domain** 命令查看 system 域下的“Login authentication scheme:”字段取值是否为“LDAP=*xx*”。如果 system 域下无“Login authentication scheme:”字段，再查看“Default authentication scheme:”字段取值是否为“LDAP=*xx*”。

如果以上配置不准确，请在相关 ISP 域下配置 Login 用户采用 LDAP 认证方案。LDAP 服务器一般只作为认证服务器，授权和计费通常配置为其它方式，比如 local、RADIUS 或 HWTACACS（下例中，认证采用 LDAP 方案 ccc、授权和计费为 local）。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login ldap-scheme ccc
[Sysname-isp-test] authorization login local
[Sysname-isp-test] accounting login local
```

(4) 通过 LDAP 的调试信息辅助排查如下故障。

执行 **debugging ldap error** 命令打开 LDAP 错误调试信息开关，可根据系统打印的如下调试信息定位问题：

- “Failed to perform binding operation as administrator.“表示 LDAP 服务器视图下配置的管理员用户 DN 不存在或管理员密码不正确。针对此问题，可以进入 LDAP 服务器视图，执行 **login-dn** 和 **login-password** 命令修改管理员用户 DN 和密码配置（下例中管理员权限的用户 DN 为 cn=administrator,cn=users,dc=ld、管理员密码为 admin!123456）。

  ```
  <Sysname> system-view
  [Sysname] ldap server ldap1
  [Sysname-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ld
  [Sysname-ldap-server-ldap1] login-password simple admin!123456
  ```

- “Failed to get bind result.errno = 115”表示对端未开启 LDAP 服务或 LDAP 服务器异常。针对此问题，可以联系 LDAP 服务器管理员解决。
- “Bind operation failed.”表示设备与 LDAP 服务器之间不可达，可以尝试排查设备和服务器中间链路不通的问题。
- “Failed to perform binding operation as user.”表示 LDAP 用户密码错误。
- “Failed to bind user *username* for the result of searching DN is NULL.”表示 LDAP 用户不存在。针对此问题，可以联系 LDAP 服务器管理员解决。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息、诊断信息。
- 打开 LDAP 调试信息开关（通过 **debugging ldap all** 命令），收集设备的调试信息。

5. 告警与日志

相关告警

模块名：HH3C-UI-MAN-MIB

- hh3cLogInAuthenFailure (1.3.6.1.4.1.25506.2.2.1.1.3.0.3)

模块名：HH3C-SSH-MIB

- hh3cSSHUserAuthFailure (1.3.6.1.4.1.25506.2.22.1.3.0.1)

相关日志

- LOGIN/5/LOGIN_AUTHENTICATION_FAILED
- LOGIN/5/LOGIN_FAILED
- SSHS/6/SSHS_AUTH_FAIL

16.3 MAC地址认证故障处理

16.3.1 MAC 地址认证失败

1. 故障描述

MAC 地址认证用户认证失败或认证异常。

2. 常见原因

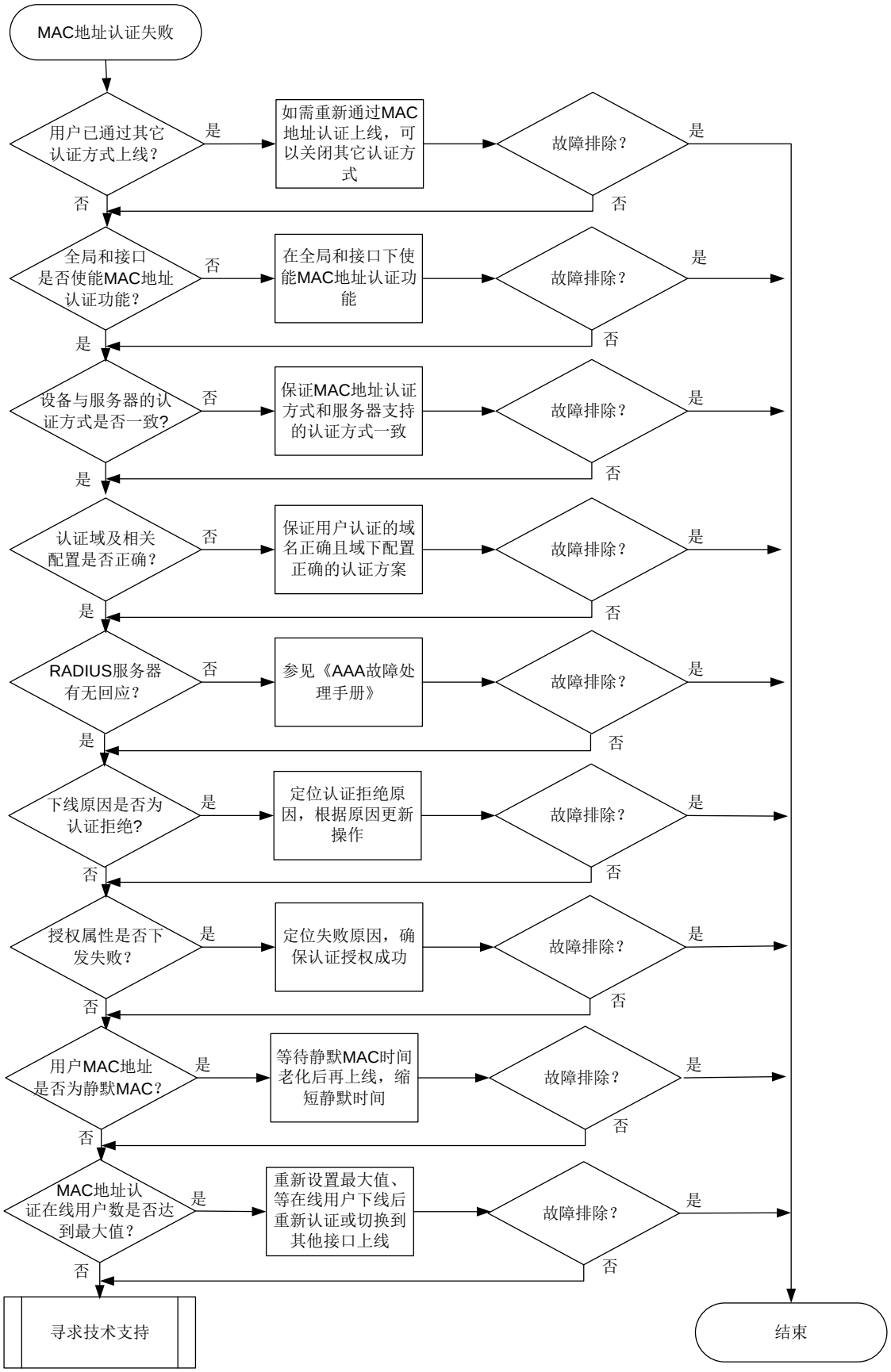
本类故障的常见原因主要包括：

- 用户已通过其它认证方式上线。
- 全局或接口 MAC 地址认证功能未开启。
- 设备配置的认证方式与 RADIUS 服务器不一致。
- MAC 地址认证用户使用的认证域及相关配置错误。
- RADIUS 服务器无回应。
- 本地认证或 RADIUS 服务器认证拒绝。
- 授权属性下发失败。
- 用户 MAC 地址被设置为静默 MAC。
- MAC 地址认证在线用户数达到最大值。

3. 故障分析

本类故障的诊断流程如图 115 所示。

图115 MAC 地址认证用户认证失败的故障诊断流程图



4. 处理步骤

注意

- Debug 开关不能在设备正常运行时随意开启，可在故障发生后复现故障场景时打开。
- 请及时保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

(1) 检查用户是否已通过其它认证方式上线。

通过 **display dot1x connection** 命令查看当前 MAC 地址是否已经通过了 802.1X 认证成功上线。如果已经在线，请判断是否需要通过 MAC 地址认证重新上线，如果需要，则将相应的 802.1X 用户下线并关闭 802.1X 认证功能，然后再尝试进行 MAC 地址认证。

(2) 检查全局或接口 MAC 地址认证功能是否开启。

a. 执行 **display mac-authentication** 命令，如果提示“MAC authentication is not configured.”，表示全局 MAC 地址认证未开启，需要在系统视图下执行 **mac-authentication** 命令。

b. 执行 **display mac-authentication** 命令，如果有全局配置信息，无接口下的配置信息显示，则需要在用户认证的接口视图下执行 **mac-authentication** 命令。

(3) 检查认证域及相关是否配置错误。

端口上接入的 MAC 地址认证用户将按照如下先后顺序选择认证域：端口上指定的认证域 > 系统视图下指定的认证域 > 系统缺省的认证域。

a. 通过在设备上执行 **display mac-authentication** 命令查看系统和认证接口下是否配置了 MAC 地址认证用户使用的认证域。

```
<Sysname> display mac-authentication
 Global MAC authentication parameters:
   MAC authentication                  : Enabled
...
   Authentication domain               : Not configured, use default domain
...
 GigabitEthernet1/0/1  is link-up
   MAC authentication                          : Enabled
   Carry User-IP                               : Disabled
   Authentication domain                       : Not configured
...
```

b. 如果认证接口下配置了 MAC 地址认证用户使用的认证域，请执行 **display domain** 命令检查认证域下的认证方案是否配置准确；如果认证接口下未配置认证域，而系统视图下配置了认证域，则同样通过 **display domain** 命令检查该认证域下的认证方案。

c. 如果认证接口和系统视图下都没有配置 MAC 地址认证用户使用的认证域，则检查缺省认证域的配置。

d. 如果不存在缺省认证域，若通过 **domain if-unknown** 命令配置了 unknown 域，则检查 unknown 域下的认证方案是否正确。

e. 如果根据以上原则决定的认证域在设备上都不存在，则用户无法完成认证。

(4) 检查 RADIUS 服务器有无响应。

请参见《AAA 故障处理》的“RADIUS 服务器无响应”进行故障定位和处理。

(5) 检查下线原因是否为认证拒绝。

服务器认证拒绝有多种原因，最常见的有服务器上未添加用户名、用户名格式不一致、用户名密码错误、RADIUS 服务器授权策略无法匹配等。在设备上通过 **debugging radius error** 命令打开 RADIUS 错误调试信息开关查看相关的 Debug 信息，并且同时可以在设备上执行 **test-aaa** 命令发起 RADIUS 请求测试，定位故障问题后，调整服务器、设备及客户端配置。

(6) 检查授权属性是否下发失败。

a. 检查设备的系统视图下是否通过 **port-security authorization-fail offline** 命令配置了授权失败用户下线功能。如果未配置授权失败用户下线功能，缺省情况下授权失败用户也可以保持在线，则用户不是因为授权失败而导致认证失败，继续定位其它可能原因。

b. 如果配置了授权失败用户下线功能，执行 **mac-authentication access-user log enable failed-login** 命令打开 MAC 地址认证上线失败日志功能，确认授权失败的属性有哪些（例如授权 ACL、VLAN）。

c. 检查 RADIUS 服务器上的授权属性设置是否正确，确保服务器下发的授权属性内容准确。

d. 通过 **display acl** 或 **display vlan** 等命令查看设备上对应的授权属性是否存在，如果不存在，需要在设备上创建相应的授权属性，确保用户能够获取到授权的信息。

(7) 检查用户的 MAC 地址是否被设置为静默 MAC。

执行 **display mac-authentication** 命令查看“Silent MAC users“字段显示的静默 MAC 信息。如果用户的 MAC 地址属于静默 MAC，则需要等待静默时间老化后，才能再次进行 MAC 地址认证。用户可通过 **mac-authentication timer quiet** 命令重新配置静默时间。

(8) 检查 MAC 地址认证用户数是否达到了最大用户数限制。

a. 执行 **display mac-authentication** 查看认证接口下的信息，“Max online users”字段为该接口下配置的最大用户数，“Current online users”字段为接口下当前在线用户数，对比两组数据判断 MAC 地址认证在线用户数是否已经达到最大值。

b. 如果已经达到最大用户数，可以执行 **mac-authentication max-user** 命令增大最多允许同时接入的 MAC 地址认证用户数。

c. 如果 MAC 地址认证的在线用户数无法再增大，则需要等其他用户下线或切换用户的接入端口。

(9) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 执行 **mac-authentication access-user log enable** 命令收集的日志信息。
- 执行 **debugging mac-authentication all**、**debugging radius all** 命令收集的调试信息。

5. 告警和日志

相关告警

无

相关日志

- MACA_ENABLE_NOT_EFFECTIVE

- MACA_LOGIN_FAILURE

16.3.2 MAC 认证用户掉线

1. 故障描述

MAC 地址认证用户认证成功在线后，异常掉线。

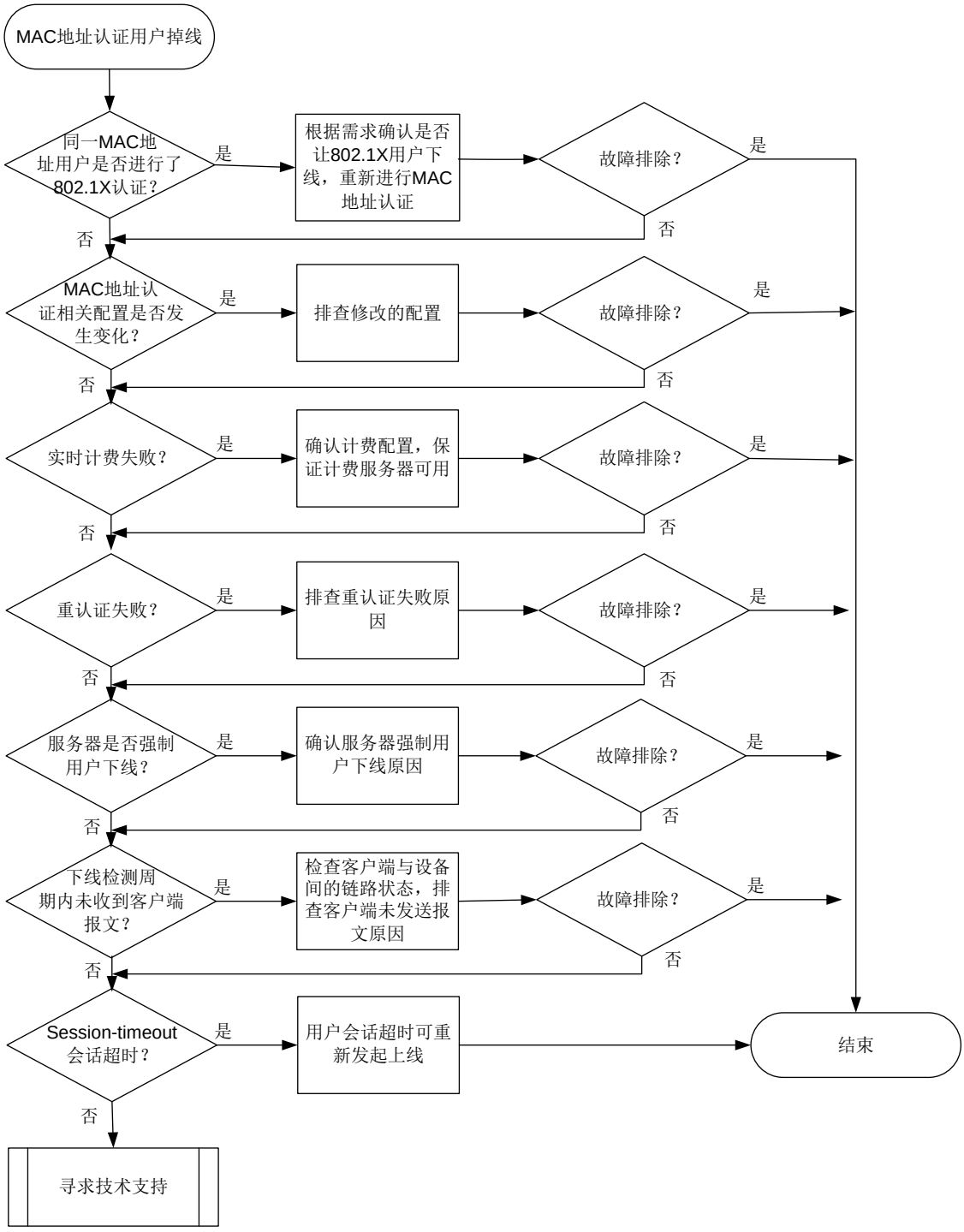
2. 常见原因

- 同一 MAC 地址的用户采用 802.1X 认证重新上线。
- 设备上 MAC 地址认证的相关配置发生变化。
- MAC 地址认证用户流量实时计费失败。
- MAC 地址认证用户重认证失败。
- 服务器强制用户下线。
- 开启下线检测后用户下线。
- 用户会话超时。

3. 故障分析

本类故障的诊断流程如图图 116所示。

图116 MAC 地址认证用户掉线的故障诊断流程图



4. 处理步骤

- Debug 开关不能在设备正常运行时随意开启，可在故障发生后复现故障场景时打开。
- 请及时保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

(1) 检查是否因为 802.1x 用户上线导致同一 MAC 地址认证用户下线。

通过 **display dot1x connection** 命令查看当前 MAC 地址是否通过了 802.1X 认证成功上线。如果已经在线，请判断是否需要通过 MAC 地址认证重新上线，如果需要，则将相应的 802.1X 用户下线并关闭接口的 802.1X 认证功能，然后再尝试进行 MAC 地址认证。

(2) 检查设备上 MAC 地址认证的相关配置是否发生变化。

a. 通过 **display mac-authentication** 命令查看设备上 MAC 地址认证的相关配置（使能开关、认证方式等）是否发生变化。

b. 通过 **display domain** 命令查看用户认证域下的配置（授权属性等）是否发生变化。

(3) 检查实时计费是否失败。

检查设备与计费服务器之间的链路状态，以及设备和计费服务器的相关计费配置是否发生过更改。

(4) 检查是否是因为重认证失败而掉线。

参考“16.3.1 MAC 地址认证失败”故障处理定位重认证失败原因。

(5) 检查是否为 RADIUS 服务器强制用户下线。

请联系服务器管理员定位服务器强制用户下线原因。

(6) 检查是否是因为下线检测定时器间隔内未收到用户报文。

检查客户端与设备之间的链路状态，排查客户端未发送报文原因。

(7) 检查用户会话是否超时。

a. 执行 **debugging radius packet** 命令打开 RADIUS 报文调试信息开关，确认服务器回应的报文中是否携带 Session-Timeout 属性。

b. 用户会话超时触发的掉线情况属于正常现象，用户可重新发起上线。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- 执行 **mac-authentication access-user log enable** 命令收集的日志信息。
- 执行 **debugging mac-authentication all**、**debugging radius all** 命令收集的调试信息。

5. 告警与日志

相关告警

无

相关日志

- MACA_LOGOFF

16.4 Password Control故障处理

16.4.1 管理员登录时系统要求修改密码

1. 故障描述

管理员采用本地认证方式登录设备时，系统判断密码强度不符合要求，提示用户修改当前的登录密码。

2. 常见原因

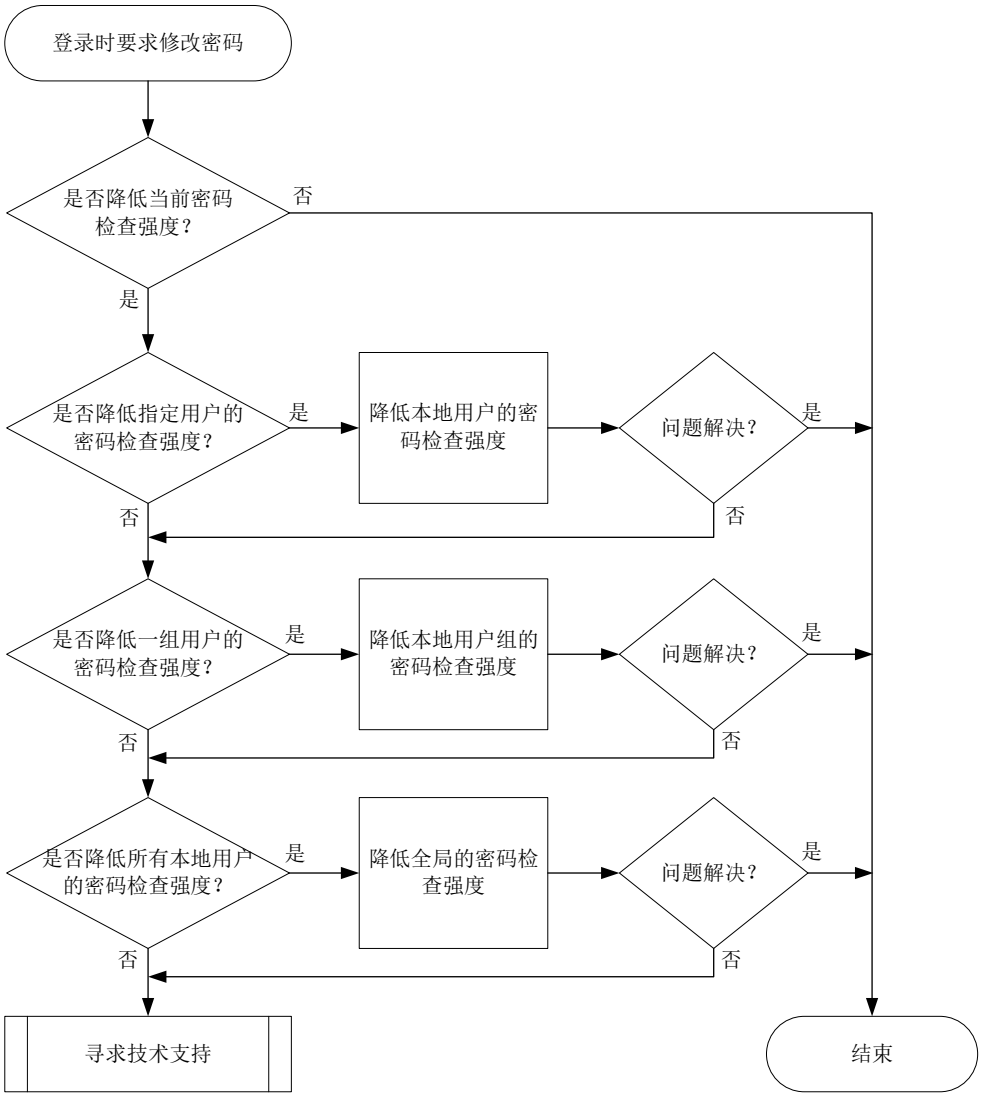
本类故障的常见原因主要包括：

- 本地用户视图下配置的 Password Control 密码检查强度高。
- 本地用户组视图下配置的 Password Control 密码检查强度高。
- 系统视图下配置的 Password Control 密码检查强度高。

3. 故障分析

本类故障的诊断流程如图 117 所示。

图117 管理员登录时要求修改密码故障诊断流程图



4. 处理步骤

(1) 判断是否降低当前密码检查强度。

开启全局密码管理功能后，通过 Telnet、SSH、HTTP、HTTPS 方式登录的设备管理类用户，输入登录密码时，系统会根据当前设定的 Password control 密码组合检测策略、密码最小长度限制以及密码复杂度检查策略检查对用户的登录密码进行检查，若不符合以上密码检查策略要求，则视为弱密码。系统缺省的密码检查策略请查看“安全配置指导”中的“Password Control”。

缺省情况下，用户使用弱密码登录设备时，系统会打印弱密码提示信息。如果当前的密码检查强度高于实际登录控制需求，请在确定修改范围（指定的本地用户、指定的用户组、所有本地用户）之后，按照如下步骤降低相应视图下的密码检查强度。

(2) 降低本地用户的 Password Control 密码检查强度。

执行 **local-user** 命令，进入本地用户视图：

- 通过 **password-control composition** 命令配置密码组合策略（下例中密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个）。
- 通过 **password-control length** 命令配置密码最小长度（下例中密码最小长度为 16 个字符）。
- 通过 **password-control complexity** 命令配置密码复杂度检查策略（下例中为检查密码中是否包含用户名）。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password-control composition type-number 4 type-length 5
[Sysname-luser-manage-test] password-control length 16
[Sysname-luser-manage-test] password-control complexity user-name check
```

(3) 降低用户组的 Password Control 密码检查强度。

执行 **user-group** 命令，进入本地用户视图：

- 通过 **password-control composition** 命令配置密码组合策略。
- 通过 **password-control length** 命令配置密码最小长度。
- 通过 **password-control complexity** 命令配置密码复杂度检查策略。

(4) 降低所有本地用户的 Password Control 密码检查强度。

在系统视图下：

- 通过 **password-control composition** 命令配置密码组合策略。
- 通过 **password-control length** 命令配置密码最小长度。
- 通过 **password-control complexity** 命令配置密码复杂度检查策略。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、诊断信息、提示信息。

5. 告警与日志

相关告警

无

相关日志

无

16.4.2 创建本地用户或配置用户密码失败

1. 故障描述

创建本地用户失败，系统打印提示信息“Add user failed.”。

配置本地用户密码失败，系统打印提示信息“Operation failed.”。

2. 常见原因

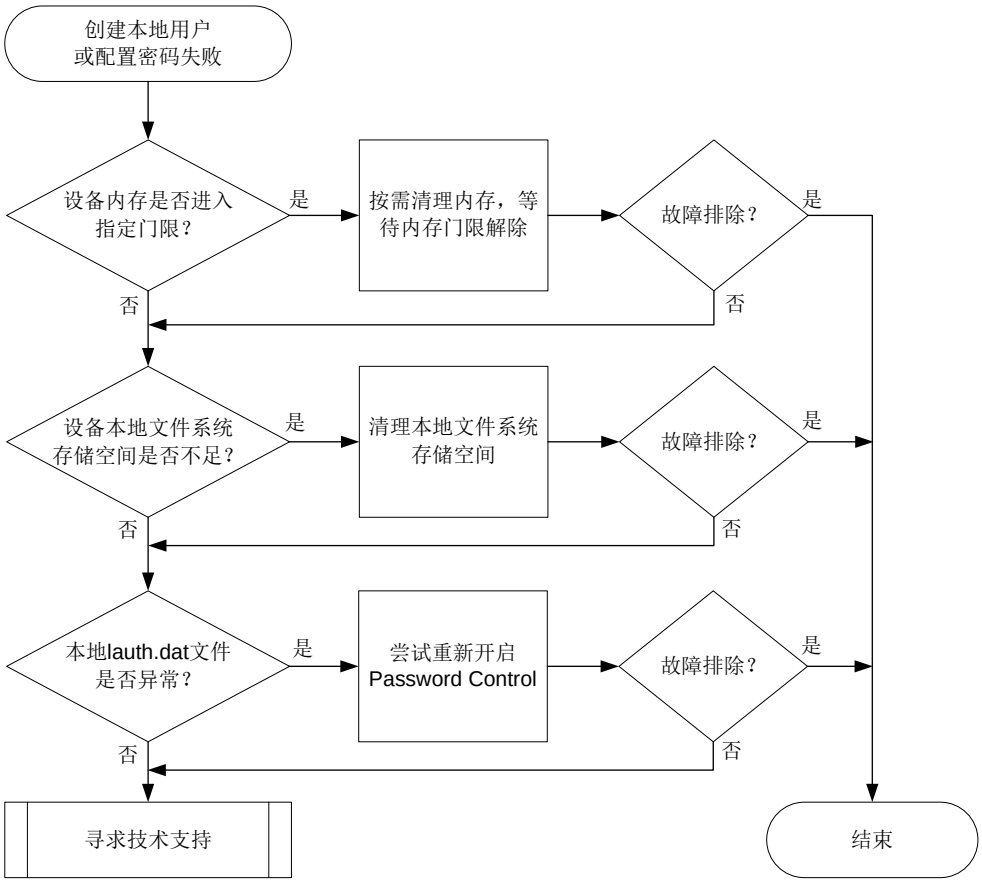
本类故障的常见原因主要包括：

- 设备的内存使用率达到指定门限。
- 设备的本地文件系统存储空间不足。
- 设备本地的 lauth.dat 文件异常。

3. 故障分析

本类故障的诊断流程如图 118 所示。

图118 创建本地用户或配置密码失败故障诊断流程图



4. 处理步骤

(1) 检查设备剩余空闲内存值是否进入指定的内存门限。

如果是修改本地用户密码失败，则无需关注内存门限问题，直接进入步骤（2）。

执行 **display memory-threshold** 命令查看显示内存告警门限相关信息，通过“Current free-memory state:”字段查看当前内存使用状态。系统内存进入一级（Minor）、二级（Severe）、三级（Critical）告警门限状态期间，不允许创建本地用户。

```
<Sysname> display memory-threshold
Memory usage threshold: 100%
Free-memory thresholds:
    Minor: 96M
    Severe: 64M
    Critical: 48M
    Normal: 128M
    Early-warning: 144M
    Secure: 160M

Current free-memory state: Normal (secure)
```

...

可在任意视图下通过执行 **monitor process** 命令查看进程统计信息，输入“m”后按照显示的内存排序定位占用内存资源过多的进程，按需进行内存清理。等待内存门限解除后，再次尝试创建本地用户。

(2) 检查设备的本地文件系统存储空间是否不足。

如果设备上输出如下日志信息，则表示文件系统异常导致此问题：

PWDCTL/6/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.

请在用户视图下执行 **dir** 命令查看本地存储介质（例如 flash）的剩余容量信息，如果剩余空间不足，则需要删除无用的文件。

(3) 检查本地 lauth.dat 文件是否正常。

开启全局密码管理功能后，设备会自动生成 lauth.dat 文件记录本地用户的认证、登录信息。如果手工删除或修改该文件，会造成本地认证异常。请在用户视图下执行 **dir** 命令查看本地存储介质中（例如 flash）的 lauth.dat 文件存在情况。

```
<Sysname> dir
Directory of flash: (EXT4)
   0 drw-           - Aug 16 2021 11:45:37   core
   1 drw-           - Aug 16 2021 11:45:42   diagfile
   2 drw-           - Aug 16 2021 11:45:57   dlp
   3 -rw-         713 Aug 16 2021 11:49:41   ifindex.dat
   4 -rw-          12  Sep 01 2021 02:40:01   lauth.dat
...
```

如果该文件不存在、大小为 0 或者很小（若小于 20B，则大概率发生了异常），请优先联系技术支持人员协助处理，若当前配置需求紧迫，可尝试重新开启全局密码管理功能来解决此问题。

```
<Sysname> system-view
[Sysname] undo password-control enable
[Sysname] password-control enable
```

以上问题解决后，请尝试重新创建本地用户或配置用户密码。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、诊断信息、提示信息。

5. 告警与日志

相关告警

无

相关日志

- PWDCTL/6/PWDCTL_FAILED_TO_WRITEPWD

16.4.3 管理员因闲置超时无法登录

1. 故障描述

管理员采用本地认证方式登录设备时，因账户闲置超时无法成功登录，系统打印提示信息“Failed to login because the idle timer expired.”。

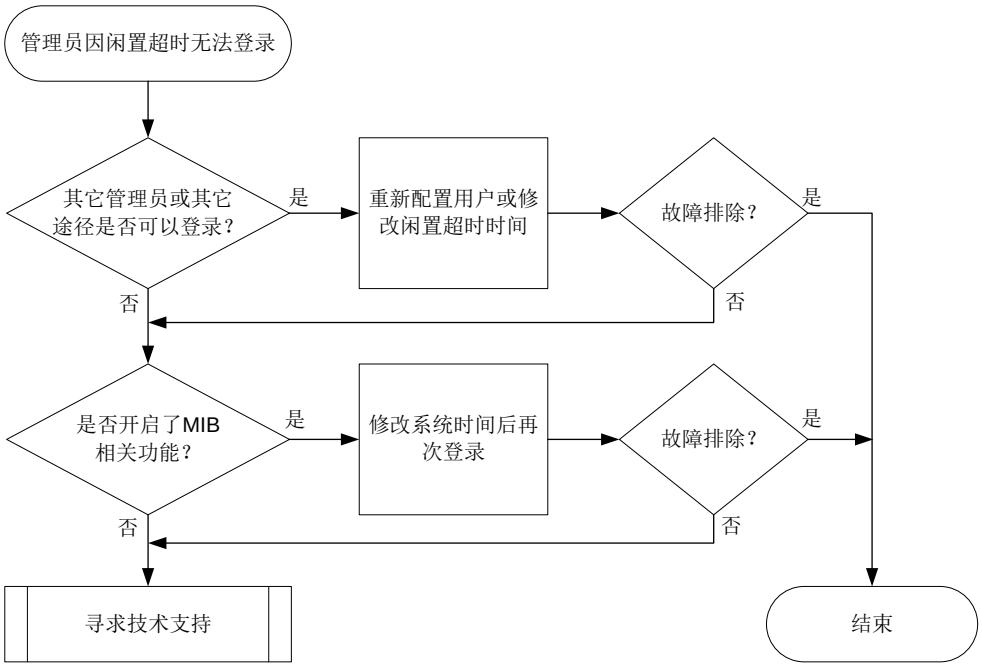
2. 常见原因

本类故障的主要原因为，用户自从最后一次成功登录之后，在配置的闲置时间内再未成功登录过，那么该闲置时间到达之后此用户账号立即失效，系统不再允许使用该账号的用户登录。

3. 故障分析

本类故障的诊断流程如图 119 所示。

图119 管理员因闲置超时无法登录故障诊断流程图



4. 处理步骤

(1) 确认是否有其它管理员或其它途径可以登录设备。

- 如果有其它管理员或其它途径（例如 Console 口）可以登录设备，则表示仅该用户被禁止登录，因此可以由其它管理员登录后删除该本地用户后重新创建此用户，或修改用户账号的闲置时间（通过 **password-control login idle-time** 命令）。若将闲置时间修改为 0，则会立即关闭闲置超时检查。
- 如果无其它管理员或其它途径可以登录设备，则执行步骤（2）。

(2) 确认设备是否开启了 SNMP 功能。

尝试是否可以通过 NMS（Network Management System，网络管理系统）登录设备：

- 若开启了 SNMP 功能，则可以使用 MIB 修改系统时间，将系统时间修改为闲置超时之前的某个时间点，再使用此管理员帐号登录设备。修改系统时间对应的 MIB 节点为 HH3C-SYS-MAN-MIB 中的 hh3cSysLocalClock (1.3.6.1.4.1.25506.2.3.1.1.1)。

管理员再次成功登录后，需要第一时间将系统时间恢复，并关闭用户账号闲置超时检查。

- 若未开启 SNMP 功能，则无法使用 MIB。可尝试重启设备，并按提示进入 BootWare 扩展段菜单后，选择跳过 console 口认证或者跳过配置文件选项来进入系统。建议在技术支持人员指导下执行此步骤。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、诊断信息、提示信息。

5. 告警与日志

相关告警

无

相关日志

无

16.5 Portal故障处理

16.5.1 Portal 认证页面无法弹出

1. 故障描述

用户访问任意非 Portal Web 服务器网页，或者直接访问 Portal Web 服务器，无法推出 Portal 登录页面。

2. 常见原因

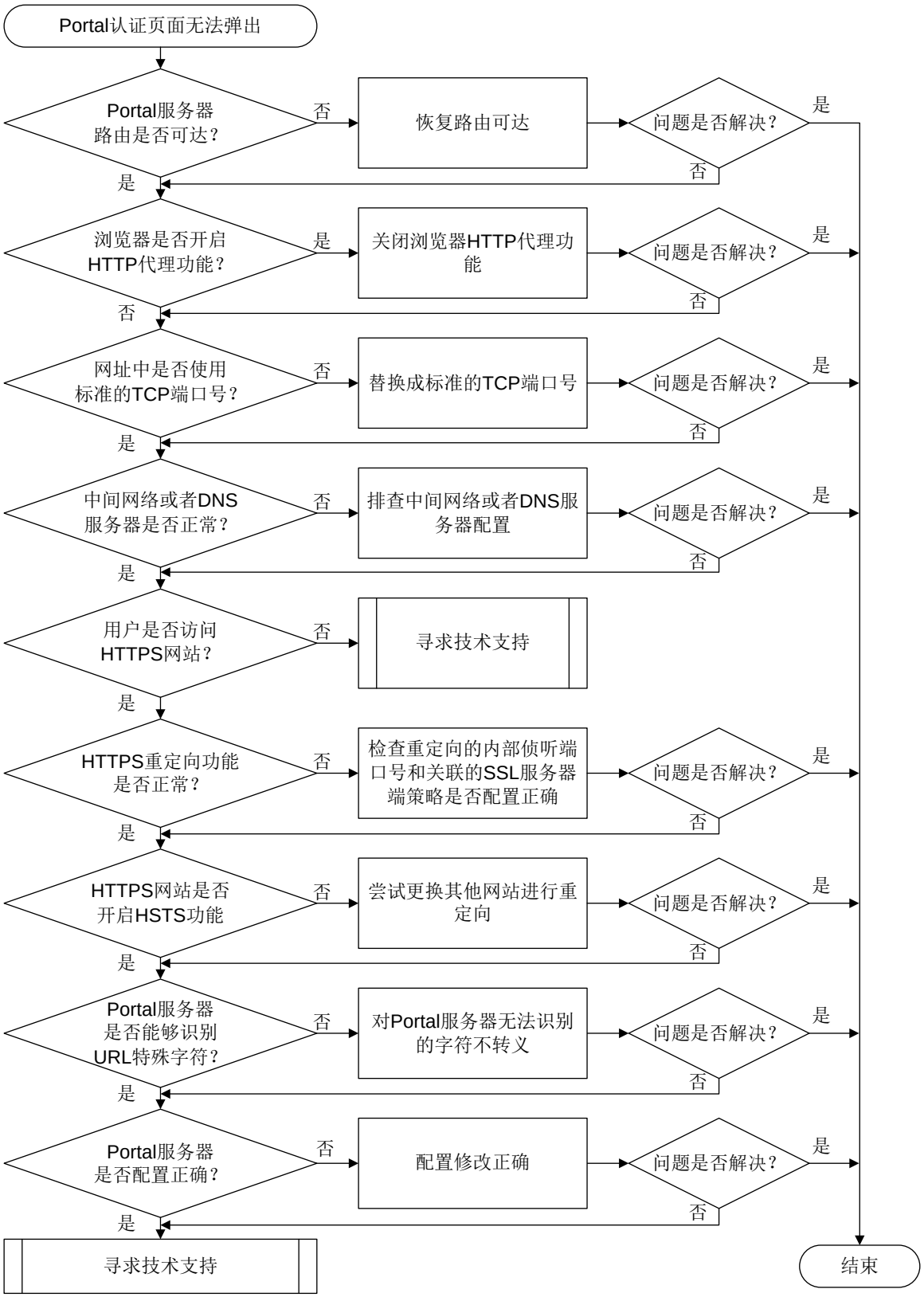
本类故障的常见原因主要包括：

- 主机、服务器和设备之间的路由不通。
- 浏览器开启了 HTTP 代理功能。
- 用户输入的网址内携带了非标准的 TCP 端口号。
- 中间网络或 DNS 服务器出现问题。
- 设备上的 HTTPS 重定向功能不能正常使用。
- 用户访问的 HTTPS 协议的网站开启了 HSTS（HTTP Strict Transport Security，HTTP 严格传输安全协议）功能。
- Portal 服务器无法识别转义后的 URL 特殊字符。
- Portal 服务器配置错误。

3. 故障分析

本类故障的诊断流程如图 120 所示：

图120 Portal 认证页面无法弹出的故障诊断流程图



4. 处理步骤

(1) 确认终端和 Portal 服务器上的路由配置是否正确。

在终端上关闭防火墙功能后，执行 Ping 操作检查 Portal 服务器是否可达，如果 Ping 不通，首先需要确认终端和 Portal 服务器上的路由配置是否正确，同时需要注意：

- Portal 服务器到终端的回程路由是否配置正确。
- 终端或者 Portal 服务器上是否存在有多个网卡。

  在有多个网卡的情况下，终端和服务器之间的流量不一定全部经过配置有 Portal 认证的网络。以 Windows 终端为例，在 cmd 窗口上执行 **`route print`** 命令查看具体的路由信息，然后确定用户的 Web 访问流量是从哪个网卡出去。

  最后，采取分段 Ping 的手段定位问题。首先从终端 Ping 网关（需要先取消认证，否则 Ping 不通），然后再从网关上 Ping 服务器。

(2) 终端的浏览器上是否开启了 HTTP 代理功能。

浏览器上开启了 HTTP 代理功能会导致用户无法访问 Portal 认证页面。以 Windows IE 浏览器为例，请打开 IE 浏览器，单击“工具”，选择“Internet 选项>连接>局域网设置>代理服务器”中，关闭 HTTP 代理功能。

(3) 输入的网址是否使用非标准 TCP 端口

非标准 TCP 端口是指非 80 或非 443 端口。用户输入的网址中若包含非标准 TCP 端口，会导致 Portal 认证页面无法弹出，例如 http://10.1.1.1:18008/。对于 HTTP 协议的网址，请使用 80；对于 HTTPS 协议的网址，请使用 443。

(4) 中间网络或 DNS 服务器出现问题。

a. 确认设备上是否将 DNS 服务器 IP 地址配置为允许访问的地址。

b. 检查中间网络连通性以及排查 DNS 服务器故障，在网关上进行流量统计（分别对连接终端下行接口和连接 DNS 服务器的上行接口）或镜像获取终端访问 DNS 服务器的报文，确认网关是否已将 DNS 请求发出，但却未收到回应报文。

(5) HTTPS 重定向功能是否开启。

a. 确认用户是否访问 HTTPS 网站。在配置内部侦听端口号之前，需确保该端口号没有被其他服务占用，请先通过 **`display tcp`** 命令查看已被占用的 TCP 端口号。

b. 检查 HTTPS 重定向服务器关联的 SSL 服务器端策略是否存在，若不存在，请完善相关配置。

(6) HTTPS 网站开启了 HSTS 功能。

HTTPS 网站开启了 HSTS 功能后，要求浏览器必须使用 HTTPS 访问，而且证书必须要合法。设备对用户浏览器进行 HTTPS 重定向时，设备会使用自签名证书（设备没有目标网站的证书，只能使用自签名证书）伪装成目标网站和浏览器建立 SSL 连接，此时浏览器一旦检测到证书不受信任，将会导致 HTTPS 重定向失败，无法弹出 Portal 认证页面。这种情况依赖于具体网站配置的 HSTS 协议的强制要求，无法解决。此时，建议用户更换其他网站进行尝试。

(7) Portal 服务器配置是否正确。

- 检查 Portal 服务器上是否配置了 IP 地址组，以及是否将设备与 IP 地址组关联。
- 检查终端 IP 地址是否在 Portal 服务器上配置的 IP 地址组范围内。

(8) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。

- 设备的配置文件、日志信息和告警信息。
- 服务器上 Portal 相关配置截图。
- 设备与服务器之间的抓包文件。
- 在浏览器上对问题现象进行截图。
- 在设备上通过 **display portal rule** 命令查看用于报文匹配的 Portal 过滤规则信息。
- 出现问题时，在设备上通过 **debugging portal** 和 **debugging ip packet** 命令收集 Debug 信息。

5. 告警与日志

相关告警

无

相关日志

无

16.5.2 Portal 认证失败

1. 故障描述

Portal 用户认证失败或者认证异常。

2. 常见原因

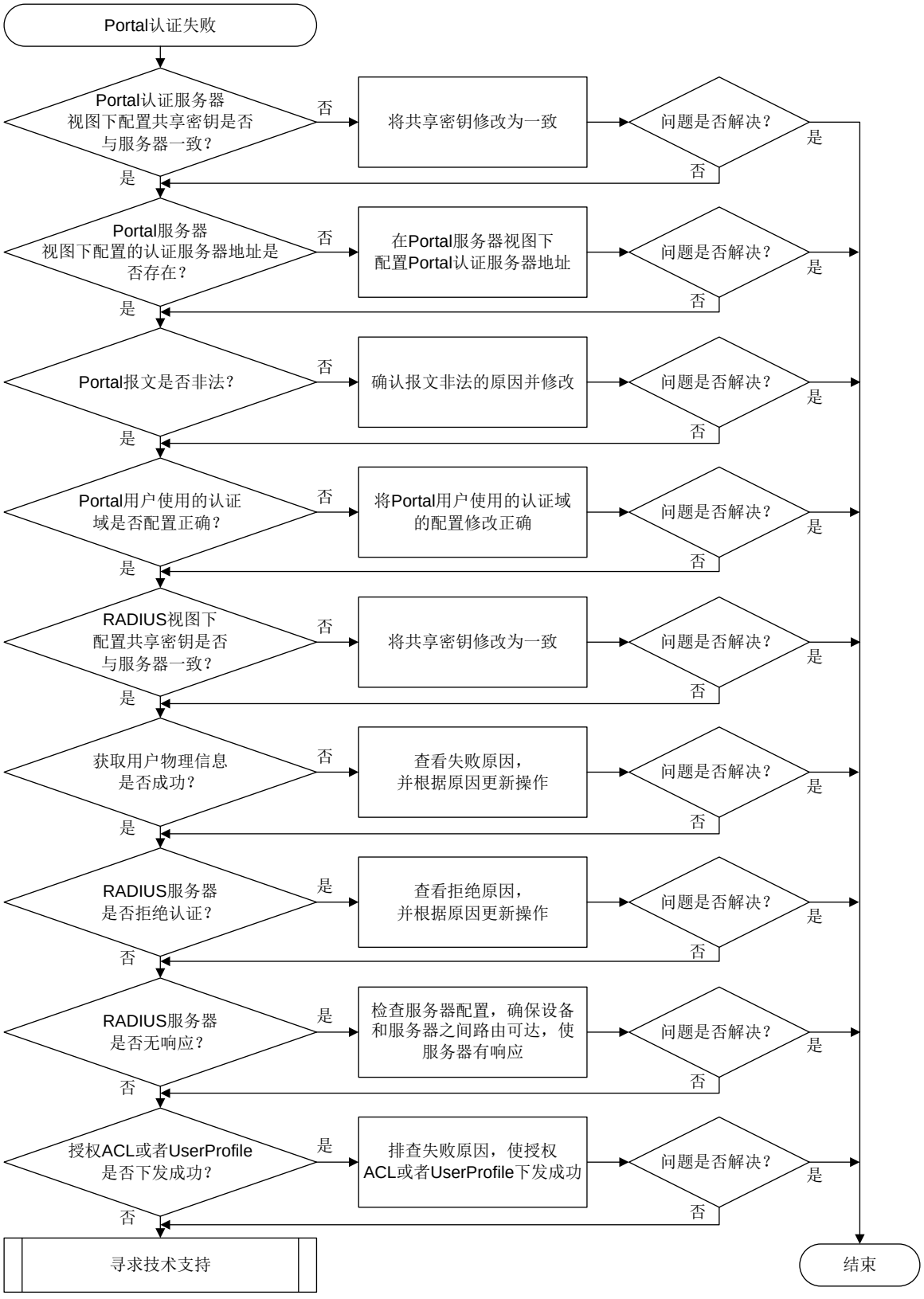
本类故障的常见原因主要包括：

- 设备上 Portal 服务器视图下配置的共享密钥和 Portal 认证服务器上配置的不一致。
- 设备上 Portal 服务器视图下配置的 Portal 认证服务器地址不存在。
- Portal 报文非法。
- Portal 用户使用的认证域配置错误。
- RADIUS 视图下配置共享密钥与 RADIUS 服务器上配置的不一致。
- 获取用户物理信息失败。
- RADIUS 服务器认证拒绝。
- RADIUS 服务器无响应。
- 授权 ACL 或者 User Profile 下发失败。

3. 故障分析

本类故障的诊断流程如图 121 所示。

图121 Portal 认证失败的故障诊断流程图



4. 处理步骤

(1) 检查设备上 Portal 服务器视图下配置的共享密钥与 Portal 认证服务器上配置的是否一致。

如图 122 所示，以 iMC 服务器为例，当输入“用户名”和“账号密码”，点击“上线”后登录界面上出现“向设备发送请求超时”的提示，表示设备上 Portal 服务器视图下配置的共享密钥有可能与服务器上配置的不一致。

图122 Portal 登录界面打印错误提示

此时，可以通过如下方法来检查：

- 在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关。如果设备上打印如下信息，则可以确认设备和 Portal 服务器配置的共享密钥不一致。

  ```
  *Jul 28 17:51:20:774 2021 Sysname PORTAL/7/ERROR: -MDC=1; Packet validity check failed due to invalid key.
  ```

- 通过 **display portal auth-error-record** 命令查看用户 Portal 认证异常记录中的 Auth error reason 字段是否显示为“Packet validity check failed due to invalid authenticator”。

如果确认不一致，请修改设备上 Portal 服务器视图下配置的共享密钥或者 Portal 认证服务器上配置的共享密钥，使其两者保持一致。

(2) 检查设备上 Portal 服务器视图下配置的 Portal 认证服务器地址是否存在。

当设备收到 Portal 服务器发送的认证报文时，设备会校验报文的源 IP 地址是否在设备上已配置的 Portal 认证服务器地址列表中。如果不在，则认为认证报文是非法报文，会将它丢弃。

如图 123 所示，以 iMC 服务器为例，当输入“用户名”和“账号密码”，点击“上线”后登录界面上出现“向设备发送请求超时”的提示，表示设备上 Portal 服务器视图下配置的 Portal 认证服务器地址可能不存在。

图123 Portal 登录界面打印错误提示

此时，可以通过如下方法来检查：

- 在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关。如果设备上打印如下信息，则可以确认设备上配置的 Portal 认证服务器 IP 地址错误。

  ```
  *Jul 28 19:15:10:665 2021 Sysname PORTAL/7/ERROR: -MDC=1;Packet source unknown.
  Server IP:192.168.161.188, VRF Index:0.
  ```

- 通过 **display portal auth-error-record** 命令查看用户 Portal 认证异常记录，查看 Auth error reason 字段中是否显示为“Packet source unknown. Server IP:X.X.X.X, VRF index:0”。

如果确认不正确，请在设备的 Portal 服务器视图下，执行 **ip** 命令修改 Portal 服务器的 IP 地址。

(3) 检查 Portal 报文是否非法。

设备收到 Portal 服务器发送的 Portal 协议报文后，会对报文做合法性校验。如果报文长度不对、报文校验段错误，则该报文将被视为非法报文而丢弃。

可以通过如下方法来检查 Portal 协议报文是否非法：

- 通过 **display portal packet statistics** 命令查看是否存在非法报文计数增长，如果存在，可通过在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关排查具体原因。
- 通过 **display portal auth-error-record** 命令查看用户 Portal 认证异常记录，查看 Auth error reason 字段是否显示为“Packet type invalid”或者“Packet validity check failed because packet length and version don't match”。

如果 Portal 协议报文非法，请确认报文非法的原因并进行修改，使 Portal 协议报文成为合法报文。

(4) 检查 Portal 用户使用的认证域配置。

Portal 用户将按照如下先后顺序选择认证域：接口或无线服务模板上指定的 Portal 用户使用的 ISP 域-->用户名中携带的 ISP 域-->系统缺省的 ISP 域。如果根据以上原则决定的认证域在设备上不存在，且设备上为未知域名的用户指定了此不存在的 ISP 域，将会导致用户将无法认证。

通过 **display portal** 命令查看认证接口上是否引用了认证域。

- 如果引用了认证域，确认设备上是否存在该认证域以及该域下的认证、授权、计费方案是否配置准确。
- 如果没有引用认证域，请检查用户名中携带的域是否存在，如果不存在，请检查是否存在缺省认证域并确认缺省域下配置是否正确。

如图 124 所示，以 iMC 为例，当输入“用户名”和“账号密码”，点击“上线”后登录界面上出现“设备拒绝请求”的提示，表示设备上认证域可能配置不正确。

图124 Portal 登录界面打印错误提示

此时，可以通过如下方法来检查：

- 在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关。如果设备上打印如下信息，则可能是设备上认证域配置错误，需要进一步排查。

  ```
  *Jul 28 19:49:12:725 2021 Sysname PORTAL/7/ERROR: -MDC=1; User-SM [21.0.0.21]: AAA processed authentication request and returned error.
  ```

- 通过 **display portal auth-fail-record** 命令查看 Auth error reason 字段是否显示为“AAA authentication failed”或“AAA returned an error”。

如果认证域配置不正确，请执行相应的命令将 Portal 用户使用的认证域配置修改正确。

(5) 检查 RADIUS 视图下配置共享密钥是否与 RADIUS 服务器上配置的一致。

如图 125 所示，以 iMC 服务器为例，当输入“用户名”和“账号密码”，点击“上线”后登录界面上出现“向设备发送请求超时”的提示，表示 RADIUS 视图下共享密钥和服务器上配置的不一致。

图125 Portal 登录界面打印错误提示

在设备上执行 **debugging radius error** 命令，打开 RADIUS 错误调试信息开关。如果设备上打印如下信息，则可以确认设备上 RADIUS 视图下配置共享密钥和 RADIUS 服务器上配置的不一致。

```
*Jul 28 19:49:12:725 2021 Sysname RADIUS/7/ERROR: -MDC=1; The response packet has an invalid Response Authenticator value.
```

当设备向 RADIUS 服务器发起认证请求时，服务器会首先对请求报文使用共享密钥进行校验，如果校验失败，服务器会通知设备校验失败。如果共享密钥配置错误，请将 RADIUS 视图下共享密钥和服务器上配置的保持一致。

(6) 检查是否获取用户物理信息失败。

用户上线过程中 Portal 会查找用户物理信息，并根据对应的物理信息确定用户所在的接口等信息。如果查找物理信息失败，则用户会上线失败。

可通过如下方式进行检查：

- 在设备上执行 **debugging portal event** 命令，打开 Portal 事件调试信息开关。如果设备上打印如下信息，表示获取用户物理信息失败。

  ```
  *Jul 28 19:49:12:725 2021 Sysname PORTAL/7/ERROR: -MDC=1; User-SM [21.0.0.21]: Failed to find physical info for ack_info.
  ```

- 通过 **display portal auth-error-record** 或者 **display portal auth-fail-record** 命令查看 Auth error reason 字段是否显示为“Failed to obtain user physical information”或“Failed to get physical information”。

确认获取用户物理信息失败后，请排查设备是否存在该认证用户的表项，如果不存在，请进一步排查具体原因。

(7) 检查 RADIUS 服务器是否认证拒绝。

a. RADIUS 服务器回应认证拒绝有多种原因，最常见的有用户名密码错误、RADIUS 服务器授权策略无法匹配等。这些问题，首先需要查看服务器端的认证日志或者在设备上通过 **debugging radius error** 命令打开 RADIUS 错误调试信息开关查看相关的 Debug 信息找到根本原因后，再调整服务器、终端或设备配置。

b. 执行 **display portal auth-fail-record** 命令，通过查看显示信息中的 Auth error reason 字段确认用户 Portal 认证失败原因。

(8) 检查 RADIUS 服务器是否无响应。

可通过如下三种方式来检查 RADIUS 服务器是否回应。

- 执行 **display radius scheme** 命令，通过 State 字段查看服务器状态。如果为 `Blocked`，则表示服务器不可用。
- 查看设备是否打印如下日志：

  ```
  RADIUS/4/RADIUS_AUTH_SERVER_DOWN: -MDC=1; RADIUS authentication server was
  blocked: server IP=192.168.161.188, port=1812, VPN instance=public.
  ```

- 在设备上执行 **debugging radius event** 命令打开 RADIUS 事件调试信息开关，如果设备上打印如下信息，表示 RADIUS 服务器无回应。

  ```
  *Jul 28 19:49:12:725 2021 Sysname RADIUS/7/evnet: -MDC=1; Reached the maximum
  retries.
  ```

确认 RADIUS 服务器无响应后，可根据如下步骤进行处理：

a. 确认服务器是否添加了设备 IP 地址。
   - 如果没有添加，请添加正确的设备 IP 地址。如果已经添加，那么需要确定服务器添加的设备 IP 地址与认证请求的源 IP 地址是否一致（设备默认出接口的 IP 地址作为向 RADIUS 服务器发送 RADIUS 报文时使用的源 IP 地址）。
   - 如果已添加，则需确认服务器上添加的设备 IP 地址必须为认证请求的源 IP 地址。

b. 确认设备和服务器上同时获取报文确认中间链路是否存在问题，例如中间网络存在防火墙，防火墙未放通 RADIUS（默认认证端口：1812）报文。如果出现大量用户无法认证，设备上的日志里出现 RADIUS 服务器 Down 记录，那么大概率是服务器或中间网络出现异常，需要逐一排查。

(9) 检查是否授权 ACL 或者 UserProfile 下发失败。

如果设备上开启了 Portal 的授权信息严格检查模式，当认证服务器下发的授权 ACL、User Profile 在设备上不存在或者设备下发 User Profile 失败时，设备将强制 Portal 用户下线。

a. 通过查看 **display portal** 命令的 Strict checking 字段确认设备上是否开启了严格检查，再根据用户需求判断是否需要开启。如果不需要，直接关闭。如果需要，请执行步骤 b。

b. 通过在设备上执行 **display acl** 或者 **display user-profile** 命令，确认 AAA 服务器是否授权了不存在的 ACL 或者 User Profile。如果不存在，请确认服务器是否需要授权或者在设备上增加相应的 ACL 或 User Profile 配置。

(10) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- **display portal auth-error-record**、**display portal auth-fail-record** 收集信息。
- Portal 服务器上 Portal 相关配置截图。

- 设备与 AAA 服务器间的抓包文件。
- 在客户端浏览器上对问题现象截图。
- 通过开启 **`debugging portal`** 命令收集调试信息。

5. 告警与日志

相关告警

无

相关日志

- RADIUS/4/RADIUS_AUTH_SERVER_DOWN

16.5.3 Portal 认证用户掉线

Portal 用户上线一段时间后掉线。

1. 常见原因

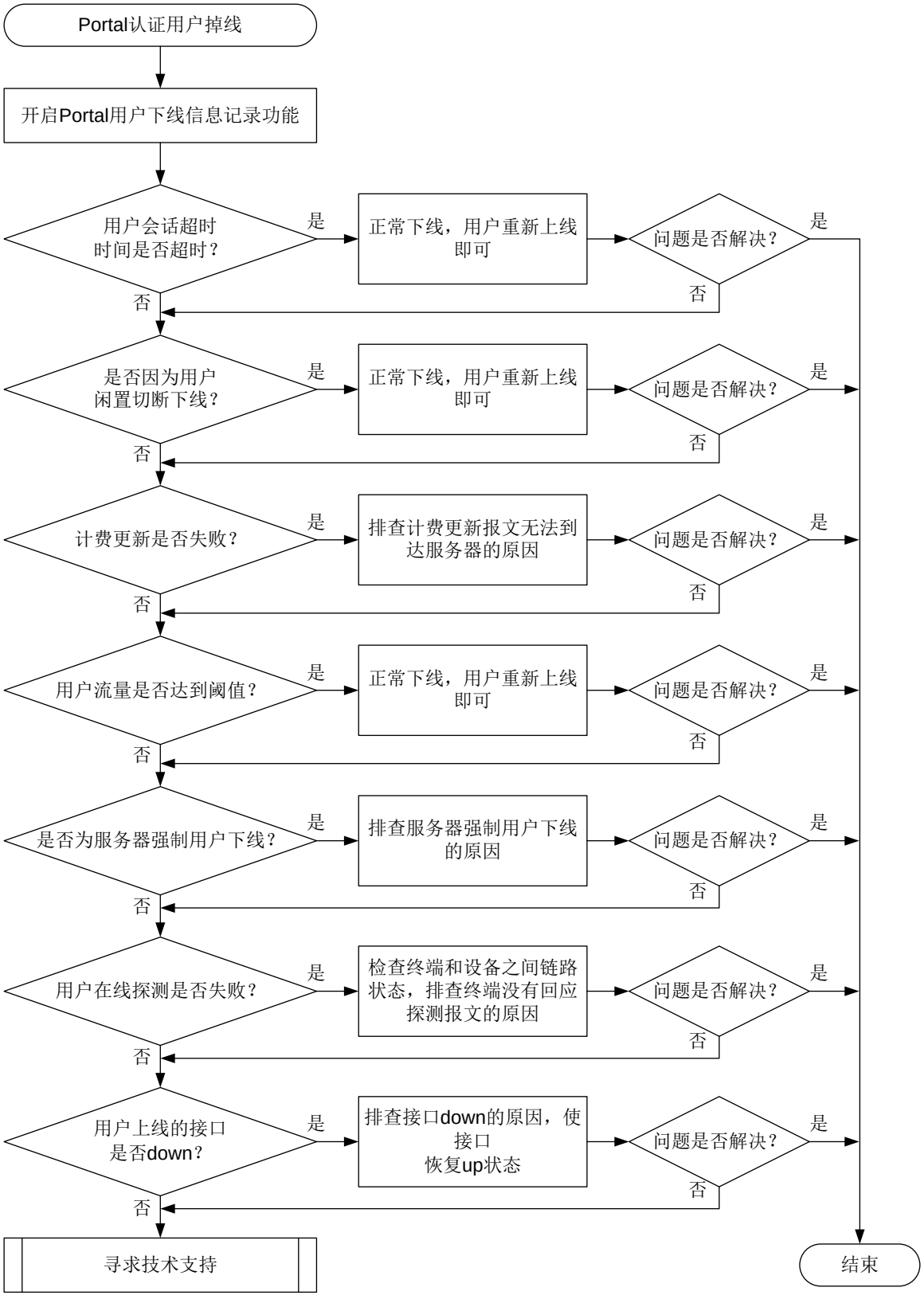
本类故障的常见原因主要包括：

- 用户会话超时时间超时。
- 用户闲置切断。
- 计费更新失败。
- 用户流量达到阈值。
- 服务器强制用户下线。
- 用户在线探测失败下线。
- 用户上线的接口 down。

2. 故障分析

本类故障的诊断流程如图 126 所示。

图126 Portal 认证用户掉线的故障诊断流程图



3. 处理步骤

(1) 通过 **portal logout-record enable** 命令，开启 Portal 用户下线信息记录功能。

(2) 检查用户会话超时时间是否超时。

如果 AAA 服务器给 Portal 用户下发了会话时长，即用户单次在线时长。用户在线时长超过会话时长后，设备会触发用户下线。

可通过如下三种方法确认是否因会话超时导致 Portal 用户下线：

- 查看 AAA 服务器上记录的用户下线记录。
- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : Session timeout
```

- 在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关。如果设备上打印如下信息，则可以确认因用户会话超时导致 Portal 用户下线。

```
*Jul 28 17:51:20:774 2021 Sysname PORTAL/7/ERROR: -MDC=1; Session timer timed out
and the user will be logged off.
```

用户会话超时触发的下线属于正常下线，用户重新上线即可。

(3) 检查是否为用户闲置切断。

如果设备或者 AAA 服务器授权了用户闲置切断时长，用户上线后，设备会周期性检测用户的流量，若某用户在指定的闲置检测时间内产生的流量小于指定的数据流量，则会被强制下线。

可通过如下三种方法确认是否因用户闲置切换功能导致 Portal 用户下线：

- 查看 AAA 服务器上记录的用户下线记录。
- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : Idle timeout
```

- 在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关。如果设备上打印如下信息，则可以确认因用户会话超时导致 Portal 用户下线。

```
*Jul 28 17:51:20:774 2021 Sysname PORTAL/7/ERROR: -MDC=1; Idle-cut timer timed out
and the user will be logged off.
```

用户闲置切断触发的下线属于正常下线，用户重新上线即可。

(4) 检查是否为计费更新失败。

远程 Portal 认证用户上线，设备会定期向 AAA 服务器发送计费更新报文。当设备与 AAA 服务器链路不通或者服务器故障时，计费更新报文会发送失败。当达到最大重传次数后，如果计费更新报文还是发送失败并且设备上配置了用户计费更新失败策略（通过 **accounting update-fail offline** 命令配置），则触发用户下线。

可通过如下方法确认是否因计费更新失败导致用户下线：

- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : Accounting update failure
```

- 通过 **display interface** 查看设备上连接 AAA 服务器的端口是否发生过变化，检查 AAA 服务器否有异常记录等。或者通过 **display radius scheme** 命令显示的 State 字段查看服务器状态是否为 Block，如果是，则可能是计费更新失败导致的下线。
- 在设备上执行 **debugging portal error** 命令，打开 Portal 错误调试信息开关。如果设备上打印如下信息，则可以确认因用户会话超时导致 Portal 用户下线。

```
*Jul 28 17:51:20:774 2021 Sysname PORTAL/7/ERROR: -MDC=1; Processed
accounting-update failed and user logout.
```

如果确认是计费更新失败导致的用户下线，请检查设备与服务器之间的链路状态，以及设备和 AAA 服务器的相关计费配置是否发生过更改。

(5) 检查是否为用户流量达到阈值。

用户上线时，如果 AAA 服务器下发了流量阈值，当用户的流量超过 AAA 服务器下发的流量阈值时，设备就会强制用户下线。

可通过如下方法确认是否因用户流量达到阈值导致用户下线：

- 查看 AAA 服务器上记录的用户下线记录。
- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
```

```
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : User traffic reached threshold
```

用户流量达到阈值触发的下线属于正常下线，用户重新上线即可。

(6) 检查是否为 AAA 服务器主动踢用户下线。

设备上开启了 RADIUS session control 功能后，若收到 AAA 服务器的断开连接请求，则会立马强制对应的用户下线。首先查看设备上是否开启了（通过 **radius session-control enable** 命令配置）。如果开启了，则可以通过如下方法查看是否因 AAA 服务器强制用户下线导致用户下线：

- 查看 AAA 服务器上记录的用户下线记录。
- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : Force logout by RADIUS server
```

服务器为何强制用户下线，请联系服务器管理员进行确认。

(7) 检查是否为 Portal 用户在线探测失败导致用户下线。

如果设备上开启了 Portal 用户在线探测功能（通过 **portal user-detect** 命令配置），设备会定期向用户终端发送探测报文。若在指定探测次数内，设备未收到终端的回应，则强制用户下线。

确认设备上是否开启了 Portal 用户在线探测功能。如果开启了，则可以通过如下方法确认是否因用户在线探测失败导致用户下线：

- 查看 AAA 服务器上记录的用户下线记录。
- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : User detection failure
```

如果确认是因 Portal 用户在线探测导致用户下线，请检查终端和设备之间的链路状态，排查终端没有回应探测报文的原因。

(8) 检查 Portal 用户上线的接口是否 down。

如果 Portal 用户上线的接口 down 了一段时间后，设备会强制从该接口接入的 Portal 用户全部下线。

可通过如下方法确认是否因接口 down 导致用户下线：

- 查看 AAA 服务器上的用户下线记录。
- 通过 **display interface** 命令查看接口的状态是否发生过变化，如果发生变化的时间正好和用户下线的时间接近，则可能是接口 down 触发的用户下线。
- 通过 **display portal logout-record** 命令查询用户下线记录。

```
<Sysname> display portal logout-record all
Total logout records: 1
User name              : gkt
User MAC               : 0800-2700-94ad
Interface              : Vlan-interface100
User IP address        : 21.0.0.20
AP                     : N/A
SSID                   : N/A
User login time        : 2021-07-29 11:05:58
User logout time       : 2021-07-29 11:05:58
Logout reason          : Interface down
```

如果确认是接口 down 导致的下线，请排查接口 down 的原因，如网线口松动等。

(9) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。
- Portal 服务器上 Portal 相关配置截图。
- AAA 服务器上记录的用户下线记录。
- 设备与服务器间的抓包文件。
- 在客户端浏览器上对问题现象截图。
- 通过开启 **debugging portal** 命令收集调试信息。

4. 告警与日志

相关告警

无

相关日志

无

17 安全类故障处理

17.1 SSH故障处理

17.1.1 SSH 客户端登录设备失败

1. 故障描述

设备作为 SSH 服务器，用户使用 SSH 客户端登录设备失败。

2. 常见原因

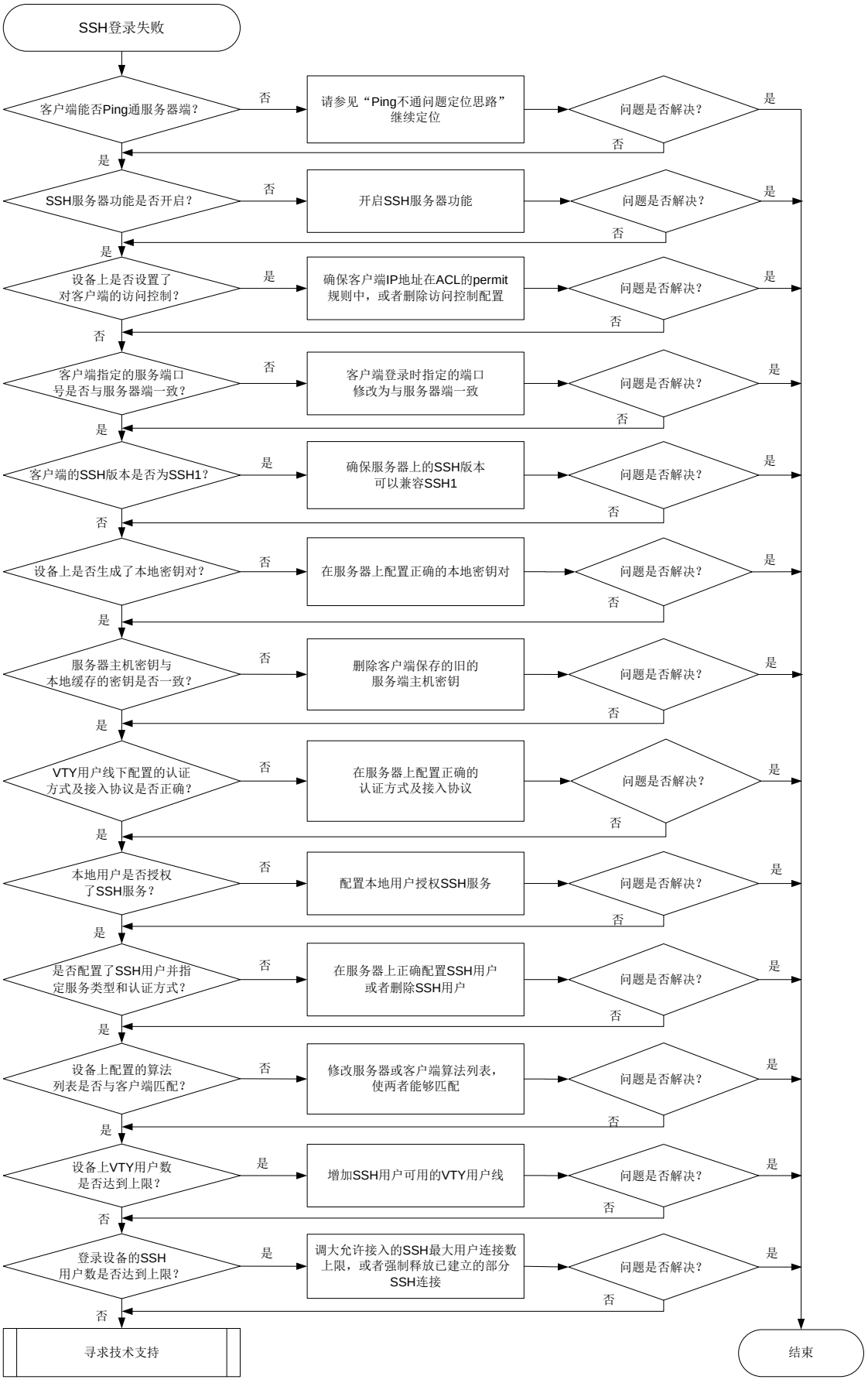
本类故障的常见原因主要包括：

- SSH 客户端与设备之间路由不通，无法建立 TCP 连接。
- 设备未开启 SSH 服务器功能。
- 设备上配置了对 SSH 客户端的访问控制，且客户端的 IP 地址不在 ACL 定义的 permit 规则范围内。
- 客户端指定的服务端口号与服务器端不一致。
- 设备上的 SSH 版本与客户端不兼容。
- 设备上未生成本地密钥对。
- 服务器主机密钥与设备上缓存的密钥不匹配。
- 用户线的认证方式或接入协议配置不正确。
- 设备上的本地用户视图下未配置 SSH 服务。
- SSH 用户的服务类型或认证方式配置不正确。
- 设备上 SSH2 协议使用的算法与客户端不匹配。
- 设备上 VTY 用户线资源不足。
- 设备上 SSH 登录用户数达到上限。

3. 故障分析

本类故障的诊断流程如图 127 所示。

图127 SSH 登录失败故障诊断流程图


SSH登录失败
客户端能否Ping通服务器端？
否
请参见“Ping不通问题定位思路”继续定位
问题是否解决？
是
否
是
SSH服务器功能是否开启？
否
开启SSH服务器功能
问题是否解决？
是
否
是
设备上是否设置了对客户端的访问控制？
是
确保客户端IP地址在ACL的permit规则中，或者删除访问控制配置
问题是否解决？
是
否
否
客户端指定的服务端口号是否与服务器端一致？
否
客户端登录时指定的端口修改为与服务器端一致
问题是否解决？
是
否
是
客户端的SSH版本是否为SSH1？
是
确保服务器上的SSH版本可以兼容SSH1
问题是否解决？
是
否
否
设备上是否生成了本地密钥对？
否
在服务器上配置正确的本地密钥对
问题是否解决？
是
否
是
服务器主机密钥与本地缓存的密钥是否一致？
否
删除客户端保存的旧的服务端主机密钥
问题是否解决？
是
否
是
VTY用户线下配置的认证方式及接入协议是否正确？
否
在服务器上配置正确的认证方式及接入协议
问题是否解决？
是
否
是
本地用户是否授权了SSH服务？
否
配置本地用户授权SSH服务
问题是否解决？
是
否
是
是否配置了SSH用户并指定服务类型和认证方式？
否
在服务器上正确配置SSH用户或者删除SSH用户
问题是否解决？
是
否
是
设备上配置的算法列表是否与客户端匹配？
否
修改服务器或客户端算法列表，使两者能够匹配
问题是否解决？
是
否
是
设备上VTY用户数是否达到上限？
是
增加SSH用户可用的VTY用户线
问题是否解决？
是
否
否
登录设备的SSH用户数是否达到上限？
是
调大允许接入的SSH最大用户连接数上限，或者强制释放已建立的部分SSH连接
问题是否解决？
是
否
否
寻求技术支持
结束

4. 处理步骤

(1) 检查客户端能否 Ping 通设备。

使用 **ping** 命令检查网络连接情况。

- 如果 Ping 不通，请参见“Ping 不通的定位思路”继续定位，确保 SSH 客户端能 Ping 通服务器端。
- 如果可以 Ping 通，请执行步骤(2)。

(2) 检查 SSH 服务器功能是否开启。

当设备上出现如下日志时，表示 SSH 服务器功能未开启。

```
SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type is not supported.
```

可以在设备上执行 **display ssh server status** 命令，检查 Stelnet 服务器功能、SFTP 服务器功能、NETCONF over SSH 服务器功能和 SCP 服务器功能是否按需开启。

```
<Sysname> display ssh server status
 Stelnet server: Disable
 SSH version : 2.0
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP Server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
```

- 如果未开启，请在设备上执行如下命令，开启相关的 SSH 服务器功能。

  ```
  <Sysname> system-view
  [Sysname] ssh server enable
  [Sysname] sftp server enable
  [Sysname] scp server enable
  [Sysname] netconf ssh server enable
  ```

- 如果已开启，请执行步骤(3)。

(3) 检查是否设置了对客户端的访问控制。

首先检查设备上是否通过 **ssh server acl** 命令设置了对客户端的访问控制。

- 如果已设置，请检查客户端的 IP 地址是否在 ACL 的 permit 规则中。

  当设备上出现如下日志时，表示客户端的 IP 地址不在 ACL 的 permit 规则中。

  ```
  SSHS/5/SSH_ACL_DENY: The SSH connection request from 181.1.1.10 was denied by ACL rule (rule ID=20).
  SSHS/5/SSH_ACL_DENY: The SSH connection request from 181.1.1.11 was denied by ACL rule (default rule).
  ```

  - 如果不在，请修改 ACL 配置，使得客户端的 IP 地址在 ACL 的 permit 规则中。如果对所有 SSH 客户端都不需要进行访问控制，请删除对客户端的访问控制。
  - 如果在，请执行步骤(4)。

- 如果未设置，请执行步骤(4)。

(4) 检查客户端指定的服务端口号是否与服务器端一致。

如果服务器端修改了 SSH 服务端口号，客户端仍然使用缺省端口号登录时，会出现登录失败。

以我司设备作为客户端为例，会出现如下错误提示信息：`Failed to connect to host 10.1.1.1 port 100.`

- 如果客户端登录时指定的端口号与服务器端不一致，请在服务器端设备上执行 **display current-configuration | inc ssh** 命令查看服务器端配置的端口号，将客户端登录时指定的端口修改为与服务器端一致。
- 如果客户端登录时指定的端口号与服务器端一致，请执行步骤(5)。

(5) 检查服务器的 SSH 版本与客户端版本是否兼容。

当设备上出现如下日志时，表示设备的 SSH 版本与客户端版本不兼容。

```
SSHS/6/SSHS_VERSION_MISMATCH: SSH client 192.168.30.117 failed to log in because of version mismatch.
```

如果使用 SSH1 版本的客户端登录设备，可以在设备上执行 **display ssh server status** 命令查看 SSH version 字段确认 SSH 版本。

- 如果 SSH version 显示为 1.99，则表示设备可以兼容 SSH1 版本的客户端，请执行步骤(6)。
- 如果 SSH version 显示为 2.0，请在设备上执行 **ssh server compatible-ssh1x enable** 命令设置设备兼容 SSH1 版本的客户端。

(6) 检查服务器上是否生成了本地密钥对。

设备作为 SSH 服务器时，必须配置本地非对称密钥对。虽然一个客户端只会采用 DSA、ECDSA 或 RSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上生成 DSA、ECDSA 和 RSA 三种密钥对。

在设备上执行 **display public-key local public** 命令查看当前设备上的密钥对信息。

- 如果 DSA、ECDSA 和 RSA 三种密钥对都不存在，请执行 **public-key local create** 命令依次进行配置。
- 如果已配置，请执行步骤(7)。

(7) 检查服务器主机密钥与客户端上缓存的服务器主机密钥对是否一致。

如果客户端首次登录服务器设备时选择保存了服务器端主机密钥，当服务器设备更新本地密钥对后，将会导致客户端认证服务端失败。

以我司设备作客户端为例，当客户端登录时，出现如下提示信息，则表示服务器主机密钥与客户端上本地缓存的密钥不一致。

```
The server's host key does not match the local cached key. Either the server administrator has changed the host key, or you connected to another server pretending to be this server. Please remove the local cached key, before logging in!
```

- 如果不一致，请执行 **undo public-key peer** 命令，删除客户端保存的旧的服务端主机密钥。
- 如果一致，请执行步骤(8)。

(8) 查看 VTY 用户线下配置的认证方式及允许接入的协议是否正确。

当客户端为 Stelnet 客户端和 NETCONF over SSH 客户端时，需要在 VTY 用户线视图下，执行 **display this** 命令查看配置的认证方式是否为 scheme、允许接入的协议是否包含 SSH。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] display this
#
line vty 0 63
```

```
 authentication-mode scheme
 user-role network-admin
 idle-timeout 0 0
#
```

- 如果认证方式或者接入协议配置不正确，请将认证方式修改为 scheme、将允许接入的协议修改为包含 SSH。
- 如果均配置正确，请执行步骤(9)。

(9) 检查本地用户是否授权了 SSH 服务。（仅针对本地认证）

在本地用户视图下，执行 **display this** 命令查看用户可以使用的服务类型是否包含 SSH。

```
[Sysname] local-user test
[Sysname-luser-manage-test] display this
#
local-user test class manage
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

- 如果不包含，请在本地用户视图下通过 **service-type** 命令修改配置。
- 如果包含，请执行步骤(10)。

如果为远程认证方式，请参见“AAA 故障处理”进行定位。

(10) 检查是否配置了 SSH 用户并指定正确的服务类型和认证方式。

SSH 支持 Stelnet、SFTP、NETCONF 和 SCP 四种用户服务类型。

首先，根据服务器采用的认证类型，根据如下规则，查看设备上是否创建正确的 SSH 用户。

- 如果服务器采用了 publickey 认证，则必须在设备上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- 如果服务器采用了 password 认证，则必须在设备上创建相应的本地用户（适用于本地认证），或在远程服务器（如 RADIUS 服务器，适用于远程认证）上创建相应的 SSH 用户。这种情况下，并不需要通过本配置创建相应的 SSH 用户，如果创建了 SSH 用户，则必须保证指定了正确的服务类型以及认证方式。
- 如果服务器采用了 keyboard-interactive、password-publickey 或 any 认证，则必须在设备上创建相应的 SSH 用户，以及在设备上创建同名的本地用户（适用于本地认证）或者在远程认证服务器上创建同名的 SSH 用户（如 RADIUS 服务器，适用于远程认证）。

接着，根据检查的结果，进行如下操作：

- 如果未创建且无需创建，请执行步骤(11)；如果未创建但有需求创建，请通过 **ssh user** 命令进行配置。
- 如果已创建，检查 SSH 用户的服务类型和认证方式。
  - SSH 用户指定的服务类型必须与客户端类型（Stelnet 客户端、SFTP 客户端、SCP 客户端和 NETCONF over SSH 客户端）相匹配，否则将会因为服务类型不匹配而登录失败。SSH 用户服务类型是否正确，通过如下方式来检查：

    以 SCP 客户端为例，如果设备上出现如下日志，表示服务类型不匹配。

    ```
    SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type
    is not supported.
    ```

请在设备系统视图下执行 **ssh user** 命令，修改 SSH 用户的服务类型。

- 请在设备上执行 **display ssh user-information** 命令，查看 SSH 服务器采用的认证方式，根据具体的认证方式检查设备上 SSH 用户的配置是否正确。

(11) 检查设备上 SSH2 协议使用的算法列表是否与客户端匹配。

通过 **display ssh2 algorithm** 命令查看当前 SSH2 协议使用的算法列表，检查客户端支持的算法是否包含在算法列表中。比如，设备上配置了不使用 CBC 相关的加密算法，但 SSH 客户端仅支持 CBC 相关加密算法，将导致该客户端无法登录服务器。

当设备上出现如下日志信息时，表示设备上 SSH2 协议使用的算法列表是否与客户端不匹配。

```
SSHS/6/SSHS_ALGORITHM_MISMATCH: SSH client 192.168.30.117 failed to log in because of encryption algorithm mismatch.
```

- 如果客户端使用的算法与设备上的算法不匹配，可通过如下两种方式进行修改：
  - 设备可以通过执行 **ssh2 algorithm cipher**、**ssh2 algorithm key-exchange**、**ssh2 algorithm mac** 或 **ssh2 algorithm public-key** 命令修改相关算法列表，增加客户端支持的算法。
  - 在客户端添加服务端支持的相关算法。
- 如果客户端使用的算法与设备上的算法能够匹配，请执行步骤(12)。

(12) 检查设备上 VTY 用户数是否达到允许用户数的上限。

SSH 用户与 Telnet 用户登录均使用 VTY 用户线，但是 VTY 用户线是有限资源。若 VTY 类型用户线都已被占用，则后续使用 Stelnet 及 NETCONF over SSH 服务的客户端将无法登录，使用 SFTP 及 SCP 服务的客户端不占用用户线资源，不受影响，仍可登录。

当设备上出现如下日志时，表示设备上 VTY 用户数已达到允许用户数的上限。

```
SSHS/6/SSHS_REACH_USER_LIMIT: SSH client 192.168.30.117 failed to log in, because the number of users reached the upper limit.
```

通过 **display line** 命令查看 VTY 用户线资源是否充足。

- 如果 VTY 用户线资源不足，可将空闲且非 scheme 认证方式的 VTY 类型用户线认证方式修改为 scheme 认证方式；若所有 VTY 类型用户线都已是 scheme 认证方式且均处于 active 状态，可执行 **free line vty** 命令强制释放 VTY 用户线，使得新的 SSH 用户能够上线。
- 如果 VTY 用户线资源充足，请执行步骤(13)。

(13) 检查登录服务器的 SSH 用户数是否达到允许用户数的上限。

通过 **display ssh server session** 命令查看服务器的会话信息，以及查看通过 **aaa session-limit ssh** 命令配置的 SSH 最大用户连接数。

当设备上出现如下日志时，表示登录服务器的 SSH 用户数已达到允许用户数的上限。

```
SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The number of SSH sessions is 10, and exceeded the limit (10).
```

- 如果 SSH 会话数已达到上限，可通过执行 **aaa session-limit ssh** 命令调大上限；如果配置的最大用户连接数已为可配置的最大值，可客户端下线空闲的 SSH 客户端，使得新的 SSH 用户能够上线。
- 如果未达上限，请执行步骤(14)。

(14) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：HH3C-SSH-MIB

- hh3cSSHVersionNegotiationFailure (1.3.6.1.4.1.25506.2.22.1.3.0.2)

相关日志

- SSHS/5/SSH_ACL_DENY
- SSHS/6/SSHS_ALGORITHM_MISMATCH
- SSHS/6/SSHS_REACH_SESSION_LIMIT
- SSHS/6/SSHS_REACH_USER_LIMIT
- SSHS/6/SSHS_SRV_UNAVAILABLE
- SSHS/6/SSHS_VERSION_MISMATCH

17.2 SSL VPN故障处理

17.2.1 浏览器无法打开 SSL VPN 页面

1. 故障描述

在浏览器中输入 SSL VPN 网关地址，无法打开 SSL VPN 网关页面。

2. 常见原因

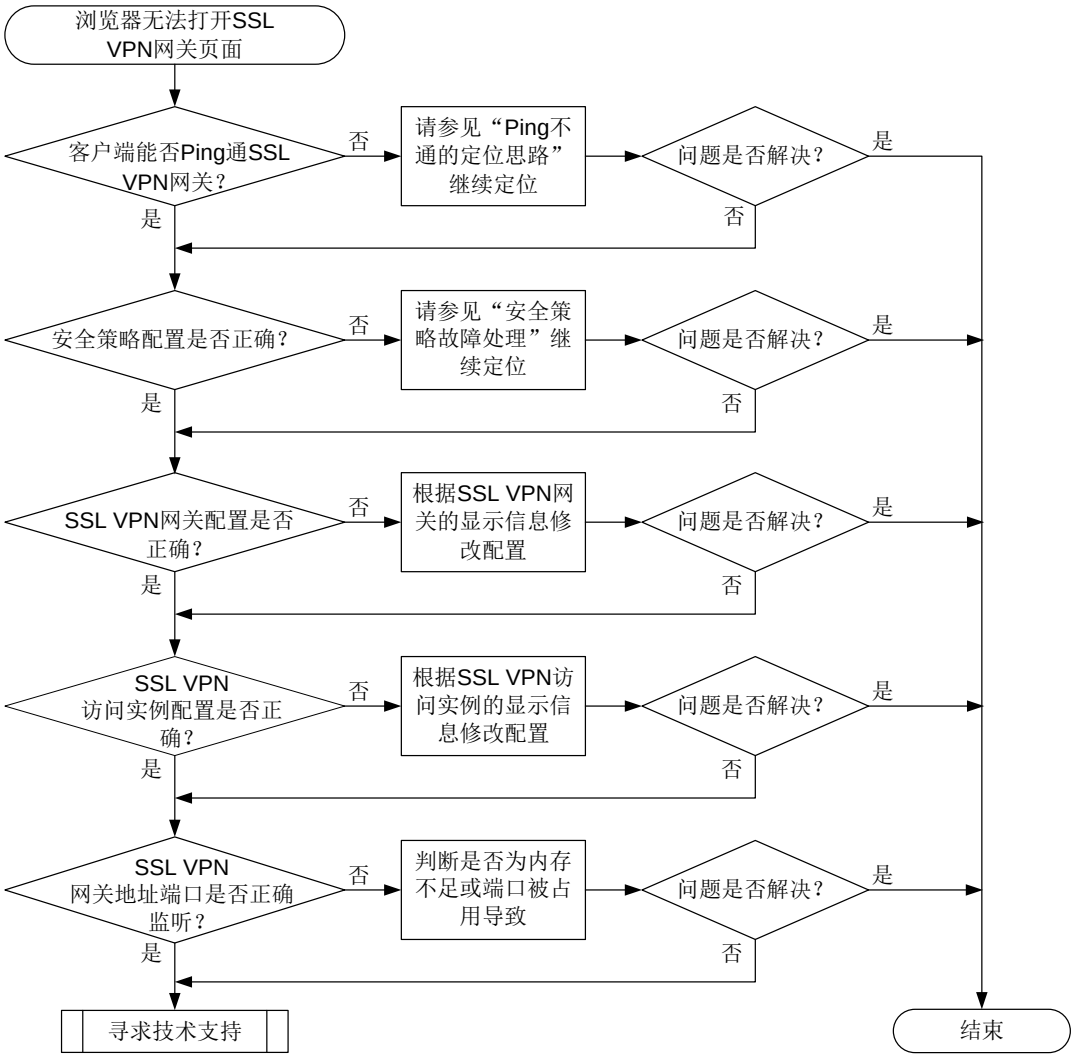
本类故障的常见原因包括：

- 客户端与 SSL VPN 网关之间路由不通，无法建立连接。
- 安全域之间的安全策略配置不正确。
- SSL VPN 网关配置不正确。
- SSL VPN 访问实例配置不正确。
- SSL VPN 网关地址和端口没有被正确监听。

3. 故障分析

本类故障的诊断流程如图 128 所示。

图128 浏览器无法打开 SSL VPN 网关页面的故障处理流程图



4. 处理步骤

(1) 检查客户端能否 Ping 通 SSL VPN 网关。

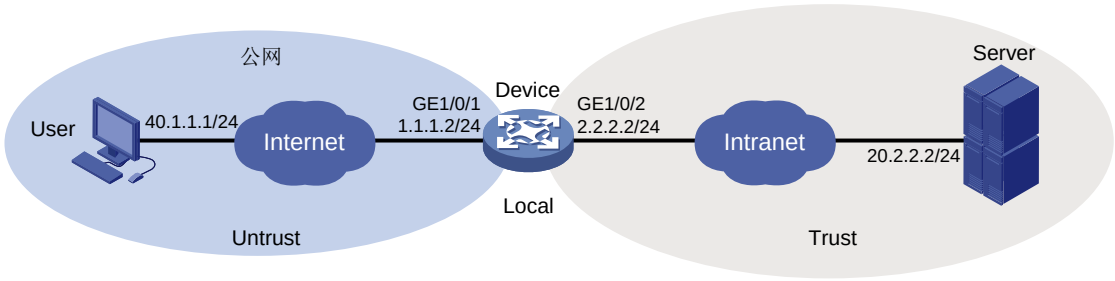
使用 **ping** 命令检查网络连接情况。

a. 如果 Ping 不通，请参见“三层技术-IP 业务类故障处理”手册中的“Ping 不通的定位思路”继续定位，确保 SSL VPN 客户端能 Ping 通 SSL VPN 网关。

b. 如果故障仍不能排除，请执行步骤(2)。

(2) 检查安全域之间的安全策略配置是否正确。

图129 SSL VPN 组网安全域示意图



如图 129 所示，在设备上查看安全域及安全策略配置信息，确保如下安全域之间的安全策略已放通：

- 确保设备本机 Local 安全域和用户所在的 Untrust 安全域互通，使得 SSL VPN 用户和 SSL VPN 网关之间可以互相发送报文。

  此安全域及安全策略相关配置信息如下：

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-Gigabitethernet 1/0/1] ip address 1.1.1.2 255.255.255.0
[Device-Gigabitethernet 1/0/1] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/1
[Device-security-zone-Untrust] quit
[Device] security-policy ip
[Device-security-policy-ip] rule name sslvpnlocalout1
[Device-security-policy-ip-1-sslvpnlocalout1] source-zone local
[Device-security-policy-ip-1-sslvpnlocalout1] destination-zone untrust
[Device-security-policy-ip-1-sslvpnlocalout1] source-ip-host 1.1.1.2
[Device-security-policy-ip-1-sslvpnlocalout1] destination-ip-host 40.1.1.1
[Device-security-policy-ip-1-sslvpnlocalout1] action pass
[Device-security-policy-ip-1-sslvpnlocalout1] quit
[Device-security-policy-ip] rule name sslvpnlocalin1
[Device-security-policy-ip-2-sslvpnlocalin1] source-zone untrust
[Device-security-policy-ip-2-sslvpnlocalin1] destination-zone local
[Device-security-policy-ip-2-sslvpnlocalin1] source-ip-host 40.1.1.1
[Device-security-policy-ip-2-sslvpnlocalin1] destination-ip-host 1.1.1.2
[Device-security-policy-ip-2-sslvpnlocalin1] action pass
[Device-security-policy-ip-2-sslvpnlocalin1] quit
[Device-security-policy-ip] quit
```

- 确保设备本机 Local 安全域和内网服务器所在的 Trust 安全域互通，使得 SSL VPN 网关和内网服务器之间可以互相发送报文。

  此安全域及安全策略相关配置信息如下：

```
[Device] interface gigabitethernet 1/0/2
[Device-Gigabitethernet 1/0/2] ip address 2.2.2.2 255.255.255.0
[Device-Gigabitethernet 1/0/2] quit
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/2
```

```
[Device-security-zone-Trust] quit
[Device-security-policy-ip] rule name sslvpnlocalout2
[Device-security-policy-ip-3-sslvpnlocalout2] source-zone local
[Device-security-policy-ip-3-sslvpnlocalout2] destination-zone trust
[Device-security-policy-ip-3-sslvpnlocalout2] source-ip-host 2.2.2.2
[Device-security-policy-ip-3-sslvpnlocalout2] destination-ip-host 20.2.2.2
[Device-security-policy-ip-3-sslvpnlocalout2] action pass
[Device-security-policy-ip-3-sslvpnlocalout2] quit
[Device-security-policy-ip] rule name sslvpnlocalin2
[Device-security-policy-ip-4-sslvpnlocalin2] source-zone trust
[Device-security-policy-ip-4-sslvpnlocalin2] destination-zone local
[Device-security-policy-ip-4-sslvpnlocalin2] source-ip-host 20.2.2.2
[Device-security-policy-ip-4-sslvpnlocalin2] destination-ip-host 2.2.2.2
[Device-security-policy-ip-4-sslvpnlocalin2] action pass
[Device-security-policy-ip-4-sslvpnlocalin2] quit
[Device-security-policy-ip] quit
```

如果故障仍不能排除，请执行步骤(3)。

(3) 检查 SSL VPN 网关配置是否正确。

通过查看 SSL VPN 网关的显示信息，确认 SSL VPN 网关的状态：

- 确认 SSL VPN 网关是否处于 Up 状态。通过执行 **display sslvpn gateway** 命令查看显示信息中 Operation state 字段的值，
- 若值为 Up，则表示 SSL VPN 网关处于 Up 状态，否则需要在 SSL VPN 网关视图下执行 **service enable** 命令开启 SSL VPN 网关，配置举例如下：

```
[Device] sslvpn gateway gw1
[Device-sslvpn-gateway-gw1] service enable
```

SSL VPN 网关的显示信息如下：

```
[Device] display sslvpn gateway
Gateway name: gw
  Operation state: Up
  IP: 1.1.1.2  Port: 2000
...
```

如果故障仍不能排除，请执行步骤(4)。

(4) 检查 SSL VPN 访问实例配置是否正确。

通过查看 SSL VPN 访问实例的显示信息，确认 SSL VPN 访问实例的状态：

- 确认 SSL VPN 访问实例是否处于 Up 状态。通过查看显示信息中 Operation state 字段的值，若值为 Up，则表示 SSL VPN 访问实例处于 Up 状态，否则需要在 SSL VPN 访问实例视图下执行 **service enable** 命令开启 SSL VPN 访问实例
- 确认 SSL VPN 访问实例是否引用了 SSL VPN 网关。通过查看显示信息中 Associated SSL VPN gateway 字段的值，若有引用的网关名称，则表示成功引用了 SSL VPN 网关，否则需要在 SSL VPN 访问实例视图下执行 gateway 命令，引用 SSL VPN 网关，配置举例如下：

```
[Device] sslvpn context ctx1
[Device-sslvpn-context-ctx1] gateway gw1
```

SSL VPN 访问实例的显示信息如下：

```
[Device] display sslvpn context
Context name: ctx
```

```
  Operation state: Up
  Associated SSL VPN gateway: gw
...
```

如果故障仍不能排除，请执行步骤(5)。

(5) 检查 SSL VPN 网关地址和端口是否被正确侦听。

通过执行 **display tcp-proxy** 命令确认 SSL VPN 网关地址和端口的侦听状态，需要分别确认每个业务板的侦听端口是否正确开启。

TCP 代理连接的显示信息如下：

```
[Device] display tcp-proxy slot 1
Local Addr:port       Foreign Addr:port     State            Service type
1.1.1.2:2000          0.0.0.0:0             LISTEN           SSLVPN
```

如果端口监听状态异常请根据如下情况进行处理：

- 由于内存不足导致：通过执行 **display memory-threshold** 命令查看设备当前内存使用状态，如果设备当前内存使用状态为告警状态，则需要等待内存空间恢复后，在 SSL VPN 网关视图下执行 undo service enable 命令关闭 SSL VPN 网关，并执行 service enable 命令重新开启 SSL VPN 网关。

  设备内存告警门限相关显示信息如下：

  ```
  [Device] display memory-threshold
  Memory usage threshold: 100%
  Free-memory thresholds:
      Minor: 256M
      Severe: 128M
      Critical: 64M
      Normal: 304M
      Early-warning: 320M
      Secure: 368M
  Current free-memory state: Minor
  ...
  ```

- 由于端口被占用导致：通过执行 **display tcp-proxy port-info** 命令查看端口使用情况，如果端口所在端口段的状态为 RESERVED，表示该端口段内的端口已被占用，需要更换 SSL VPN 网关的端口后，在 SSL VPN 网关视图下执行 undo service enable 命令关闭 SSL VPN 网关，并执行 service enable 命令重新开启 SSL VPN 网关。

  TCP 代理端口使用情况显示信息如下：

  ```
  [Device] display tcp-proxy port-info
  Index  Range            State
  16     [1024, 1087]     USABLE
  17     [1088, 1151]     USABLE
  18     [1152, 1215]     RESERVED
  19     [1216, 1279]     USABLE
  20     [1280, 1343]     USABLE
  ...
  ```

如果故障仍不能排除，请执行步骤(6)。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。

- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

17.2.2 浏览器无法登录 SSL VPN 网关

1. 故障描述

浏览器可以打开 SSL VPN 网关页面，但是无法登录。

2. 常见原因

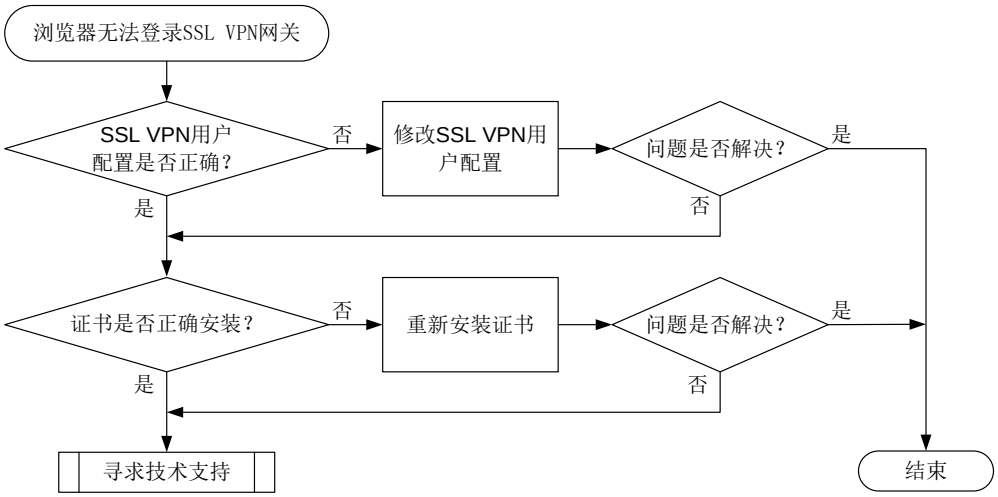
本类故障的常见原因包括：

- SSL VPN 用户配置不正确。
- 开启了客户端和服务器端证书认证，证书安装不正确。

3. 故障分析

本类故障的诊断流程如图 130 所示。

图130 浏览器无法登录 SSL VPN 网关的故障处理流程图



4. 处理步骤

(1) 检查 SSL VPN 用户配置是否正确。

针对不同的用户类型，检查用户配置。

- 本地用户：通过执行 **display local-user** 命令查看本地用户配置信息，确保用户类型为网络接入类（本地用户名称前有 Network access user 字样），服务类型为 SSL VPN（Service type 字段取值为 SSL VPN），且为 SSL VPN 用户配置资源组（SSL VPN policy group 字段有取值）。

```
<Sysname> display local-user
Network access user sslvpn:
```

```
  State:                      Active
  Service type:               SSL VPN
  User group:                 system
  Authorization attributes:
    Work directory:           flash:
    User role list:           network-operator
    SSL VPN policy group:     pg
...
```

- 远程用户：确保在设备上配置了本地用户组，且本地用户组的名称需要与远程认证服务器上用户隶属的用户组名称相同，例如，远程认证服务器上用户隶属的用户组名称和本地用户组名称同为 sslvpn。同时，需要在本地用户组内引用了 SSL VPN 策略组，该策略组在 SSL VPN policy group 字段中显示。

```
<Sysname> display user-group all
Total 1 user groups matched.

User group: sslvpn
  Authorization attributes:
    Work directory:           flash:/
    SSL VPN policy group:     policygroup1
...
```

如果故障仍不能排除，请执行步骤(2)。

(2) 检查是否正确安装了证书。

若开启了客户端和服务器端证书认证，需要确保客户端和服务器端已正确安装证书。

- 客户端证书认证：通过执行 **display ssl client-policy** 命令查看 SSL 客户端策略配置信息，检查 SSL 版本、引用的 PKI 域等配置是否正确。

```
<Sysname> display ssl client-policy policy1
 SSL client policy: policy1
     SSL version: SSL 3.0
     PKI domain: client-domain
     Preferred ciphersuite:
         RSA_AES_128_CBC_SHA
     Server-verify: enabled
...
```

- 服务器端证书认证：通过执行 **display ssl server-policy** 命令查看 SSL 服务端策略配置信息，检查 SSL 版本、引用的 PKI 域等配置是否正确。

```
<Sysname> display ssl server-policy policy1
 SSL server policy: policy1
     Version info:
         SSL3.0: Disabled
         TLS1.0: Enabled
         TLS1.1: Disabled
         TLS1.2: Enabled
         TLS1.3: Enabled
         GM-TLS1.1: Disabled
     PKI domains: server-domain
...
```

如果故障仍不能排除，请执行步骤(3)。

(3) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

17.3 IPsec故障处理

17.3.1 配置 IKE 野蛮模式的 IPsec，IPsec SA 无法协商成功

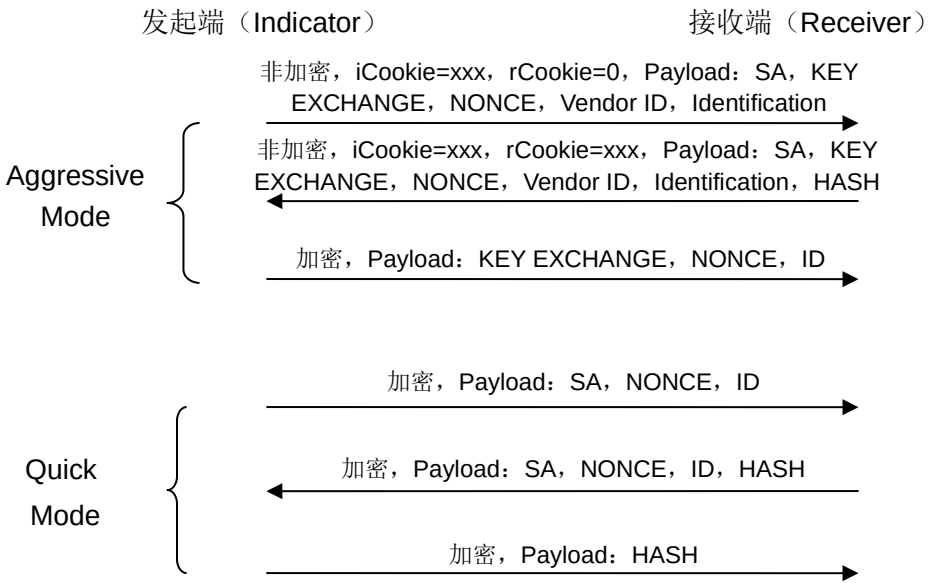
1. 故障描述

在 MSR G1 设备与 MSR G2 设备之间建立 IPsec 隧道，IKE 第一阶段的协商模式为野蛮模式，其中 MSR G1 作为发起端，MSR G2 作为接收端。通过 **display ike sa** 命令查看当前的 IKE SA 信息，发现 IKE SA 协商成功，其状态（Flags 字段）为 RD。但是通过 **display ipsec sa** 命令查看当前的 IPsec SA 时却发现没有协商出相应的 IPsec SA。

```
<Router>display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    2               10.1.1.1              RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<Router>display ipsec sa
<Router>
```

2. 故障处理步骤

野蛮模式的交互过程如下：



(1) 检查发起端 MSR G1 的所有 IKE 调试信息。

执行 **debugging ike all** 命令打开发起端 MSR G1 的所有 IKE 调试信息开关，确认协商过程中报文交互是否正常。

MSR G1 上打印的关键 debug 信息如下：

```
*Nov  7 09:23:08:808 2014 ROUTER IKE/7/DEBUG: send message: （发起端发送第一个协商报文）
*Nov  7 09:23:08:808 2014 ROUTER IKE/7/DEBUG:   ICOOKIE: 0xb8a20d7c014806fa
*Nov  7 09:23:08:808 2014 ROUTER IKE/7/DEBUG:   RCOOKIE: 0x0000000000000000
……
*Nov  7 09:23:09:365 2014 ROUTER IKE/7/DEBUG: exchange state machine(I): finished step 0, advancing...
*Nov  7 09:23:09:415 2014 ROUTER IKE/7/DEBUG: received message: （收到对端回复的第二个报文）
*Nov  7 09:23:09:516 2014 ROUTER IKE/7/DEBUG:   ICOOKIE: 0xb8a20d7c014806fa
*Nov  7 09:23:09:566 2014 ROUTER IKE/7/DEBUG:   RCOOKIE: 0x67a9145eb46c41d9
……
*Nov  7 09:23:13:510 2014 ROUTER IKE/7/DEBUG: exchange state machine(I): finished step 1, advancing...
……
*Nov  7 09:23:14:820 2014 ROUTER IKE/7/DEBUG: send message: （发送第三个协商报文）
*Nov  7 09:23:14:920 2014 ROUTER IKE/7/DEBUG:   ICOOKIE: 0xb8a20d7c014806fa
*Nov  7 09:23:14:971 2014 ROUTER IKE/7/DEBUG:   RCOOKIE: 0x67a9145eb46c41d9
……
*Nov  7 09:23:15:524 2014 ROUTER IKE/7/DEBUG: exchange state machine(I): finished step 2, advancing...（第一阶段协商完毕）
……
*Nov  7 09:23:21:801 2014 ROUTER IKE/7/DEBUG: send message: （发送第二阶段第一个报文）
*Nov  7 09:23:21:902 2014 ROUTER IKE/7/DEBUG:   ICOOKIE: 0xb8a20d7c014806fa
*Nov  7 09:23:22:002 2014 ROUTER IKE/7/DEBUG:   RCOOKIE: 0x67a9145eb46c41d9
……
```

```
*Nov  7 09:23:22:506 2014 ROUTER IKE/7/DEBUG: exchange state machine(I): finished step
0, advancing...
*Nov  7 09:23:22:606 2014 ROUTER IKE/7/DEBUG: received message: （收到对端回复的报文）
*Nov  7 09:23:22:657 2014 ROUTER IKE/7/DEBUG:   ICOOKIE: 0xb8a20d7c014806fa
*Nov  7 09:23:22:757 2014 ROUTER IKE/7/DEBUG:   RCOOKIE: 0x67a9145eb46c41d9
……
*Nov  7 09:23:24:571 2014 ROUTER IKE/7/DEBUG: validate payload NOTIFY
*Nov  7 09:23:24:621 2014 ROUTER IKE/7/DEBUG:   DOI: IPSEC
*Nov  7 09:23:24:722 2014 ROUTER IKE/7/DEBUG:   PROTO: IPSEC_ESP
*Nov  7 09:23:24:822 2014 ROUTER IKE/7/DEBUG:   SPI_SZ: 4
*Nov  7 09:23:24:873 2014 ROUTER IKE/7/DEBUG:   MSG_TYPE: INVALID_ID_INFORMATION（回
复的报文类型，协商失败）
*Nov  7 09:23:24:973 2014 ROUTER IKE/7/DEBUG: exchange setup(R): 9c16530
*Nov 7 09:23:25:024 2014 ROUTER IKE/7/DEBUG: exchange check: checking for required INFO
*Nov 7 09:23:25:124 2014 ROUTER IKE/7/DEBUG: got NOTIFY of type INVALID_ID_INFORMATION
```

从 MSR G1 打印的 debug 信息中可以看出，第一阶段的 IKE 协商交互的三个报文均正常，但是在发起端 MSR G1 发送完第二阶段协商的第一个报文后，收到了对端回复的一个 INVALID_ID_INFORMATION 的报文，导致 IPsec 协商无法继续进行。

(2) 检查接收端 MSR G2 的所有 IKE 调试信息。

执行 **debugging ike all** 命令打开接收端 MSR G2 的所有 IKE 调试信息开关，确认协商过程中报文交互是否正常。

MSR G2 上打印的关键 debug 信息如下：

```
*Nov  6 17:03:05:527 2014 ROUTER IKE/7/Event: IKE thread 366519722672 processes a job.
*Nov  6 17:03:05:527 2014 ROUTER IKE/7/Packet: Begin a new phase 1 negotiation as
responder.
*Nov 6 17:03:05:527 2014 ROUTER IKE/7/Event: Responder created an SA for peer 10.1.1.1,
local port 500, remote port 500.
*Nov  6 17:03:05:527 2014 ROUTER IKE/7/Event: Set IKE SA state to IKE_P1_STATE_INIT.
*Nov  6 17:03:05:527 2014 ROUTER IKE/7/Packet: Received ISAKMP Security Association
Payload.（收到对端发起的第一个协商报文）
……
*Nov  6 17:03:05:527 2014 ROUTER IKE/7/Packet: The profile 1 is matched.（匹配到了 ike
profile 1）
…….
*Nov 6 17:03:05:528 2014 ROUTER IKE/7/Event: Found pre-shared key in keychain 1 matching
address 10.1.1.1.（匹配到了 key chain）
…….
*Nov 6 17:03:05:535 2014 ROUTER IKE/7/Event: IKE SA state changed from IKE_P1_STATE_INIT
to IKE_P1_STATE_SEND2.
*Nov  6 17:03:05:535 2014 ROUTER IKE/7/Packet: Sending packet to 10.1.1.1 remote port
500, local port 500.（发送第二个协商报文）
……..
*Nov 6 17:03:05:739 2014 ROUTER IKE/7/Packet: Received packet from 10.1.1.1 source port
500 destination port 500.（接收到第三个协商报文）
…….
*Nov  6 17:03:05:741 2014 ROUTER IKE/7/Event: IKE SA state changed from
IKE_P1_STATE_SEND2 to IKE_P1_STATE_ESTABLISHED.（第一阶段协商完成）
*Nov  6 17:03:05:741 2014 ROUTER IKE/7/Event: Add tunnel, alloc new tunnel with ID [1].
```

```
*Nov  6 17:03:05:983 2014 ROUTER IKE/7/Packet: Received packet from 10.1.1.1 source port
500 destination port 500.（接收到第 2 阶段第 1 个报文）
…….
*Nov  6 17:03:05:984 2014 ROUTER IKE/7/Event: IPsec SA state changed from
IKE_P2_STATE_INIT to IKE_P2_STATE_GETSP.
*Nov  6 17:03:05:985 2014 ROUTER IKE/7/Error: Failed to get IPsec policy for phase 2
responder. Delete IPsec SA.
*Nov  6 17:03:05:985 2014 ROUTER IKE/7/Error: Failed to negotiate IPsec SA. （没有找
到 ipsec policy，协商失败）
*Nov  6 17:03:05:985 2014 ROUTER IKE/7/Event: Delete IPsec SA.
*Nov  6 17:03:05:985 2014 ROUTER IKE/7/Packet: Encrypt the packet.
*Nov  6 17:03:05:985 2014 ROUTER IKE/7/Packet: Construct notification packet:
INVALID_ID_INFORMATION.
*Nov  6 17:03:05:985 2014 ROUTER IKE/7/Packet: Sending packet to 10.1.1.1 remote port
500, local port 500.（知会对方协商失败。）
```

从 MSR G2 打印的 debug 信息可以看出，接收端 MSR G2 没有找到匹配的 IPsec 安全策略，这是 IPsec SA 没有协商成功的关键原因。

(3) 检查接收端 MSR G2 的 IPsec 安全策略配置。

此 IPsec 安全策略相关配置信息如下：

```
ipsec policy hzbank 7000 isakmp
transform-set 1
security acl 3000
ike-profile 1
reverse-route dynamic
reverse-route tag 10
```

从 MSR G2 打印的 IPsec 安全策略信息可以看出，接收端 MSR G2 没有在 IPsec 安全策略下配置对端的 IP 地址。

通过执行 **remote-address** 命令指定 MSR G2 的对端 IP 地址。

```
[Router]ipsec policy hzbank 7000 isakmp
[Router-ipsec-policy-isakmp-hzbank-7000]remote-address 10.1.1.1
```

说明

对于 IPsec 安全策略视图下的 **remote-address** 命令，IKE 协商发起端必须配置 IPsec 隧道的对端 IP 地址，对于使用 IPsec 安全策略模板的响应方可选配。响应方如果没有使用模板方式，也必须要配置该地址。

(4) 检查 IPsec 安全提议的配置，核对发起端 MSR G1 和接收端 MSR G2 两端配置的加密算法、认证算法等是否一致。

(5) 检查发起端 MSR G1 和接收端 MSR G2 的 IPsec 安全策略保护的数据流是否一致。

发起端 MSR G1 的 ACL 配置信息如下：

```
acl number 3001
 rule 5 permit ip source 168.201.0.0 0.0.0.7 destination 168.68.2.200 0
 rule 25 permit ip source 168.201.0.0 0.0.0.7 destination 168.201.255.1 0
```

接收端 MSR G2 的 ACL 配置信息如下：

```
acl number 3000
```

```
 rule 7 permit ip source 168.68.2.200 0 destination 168.201.0.0 0.0.127.255
```

从发起端 MSR G1 和接收端 MSR G2 两端的 ACL 信息可以看出，发起端 MSR G1 有一条流 168.201.0.0/29 -> 168.201.255.1 在接收端 MSR G2 上没有对应，导致两端的 ACL 数据流不一致。

修改接收端的 ACL 配置如下：

```
acl number 3000
rule 7 permit ip source 168.68.2.200 0 destination 168.201.0.0 0.0.127.255
rule 10 permit ip source 168.201.255.1 0 destination 168.201.0.0 0.0.127.255
```

在接收端 MSR G2 上增加了 168.201.255.1 -> 168.201.0.0/29 数据流后，IPsec 协商成功。

说明

非模板方式下，IPsec 安全策略配置中必须指定所要保护的数据流，并且要和对端所保护的数据流对应起来。例如，A、B 之间进行 IKE 协商，B 的配置中所保护的数据流是“b->a”，那么 A 上 IPsec 安全策略中指定引用的 ACL 就应该定义为“a->b”，否则会 IKE 协商失败。

准确来说，IKE 协商的发起端要保护的数据流，必须是接收端所配置的保护的数据流镜像后的子集。虽然两者保护的数据流并不是完全镜像，但是由于发起端的范围是接收端的子集，也可以协商成功。

如果发起端保护了多条数据流（即有多条 rule），那么要求所有的数据流在接收端都必须包含才可以协商成功。

模板方式下要保护的数据流是选配的。如果没有配置，那么自动使用发起端的数据流；如果配置了，要求配置的数据流范围必须包含发起端的数据流范围。

3. 故障诊断命令

命令	说明
display ike sa [**verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address* [**vpn-instance** *vpn-name*]]]	显示当前IKE SA的详细信息
display ipsec sa [**brief** | **count** | **interface** *interface-type interface-number* | { **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *profile-name* | **remote** [**ipv6**] *ip-address*]	显示安全联盟的相关信息
debugging ike error	IKE错误调试信息开关
debugging ike event	IKE消息包调试信息开关
debugging ike packet	IKE报文调试信息开关
debugging ike all	IKE所有调试信息开关
debugging ipsec all	IPsec所有调试信息开关

18 系统管理类故障处理

18.1 NETCONF故障处理

18.1.1 SOAP 方式登录失败

1. 故障描述

设备作为 NETCONF 服务器，用户使用 NETCONF over SOAP 客户端登录设备失败。

2. 常见原因

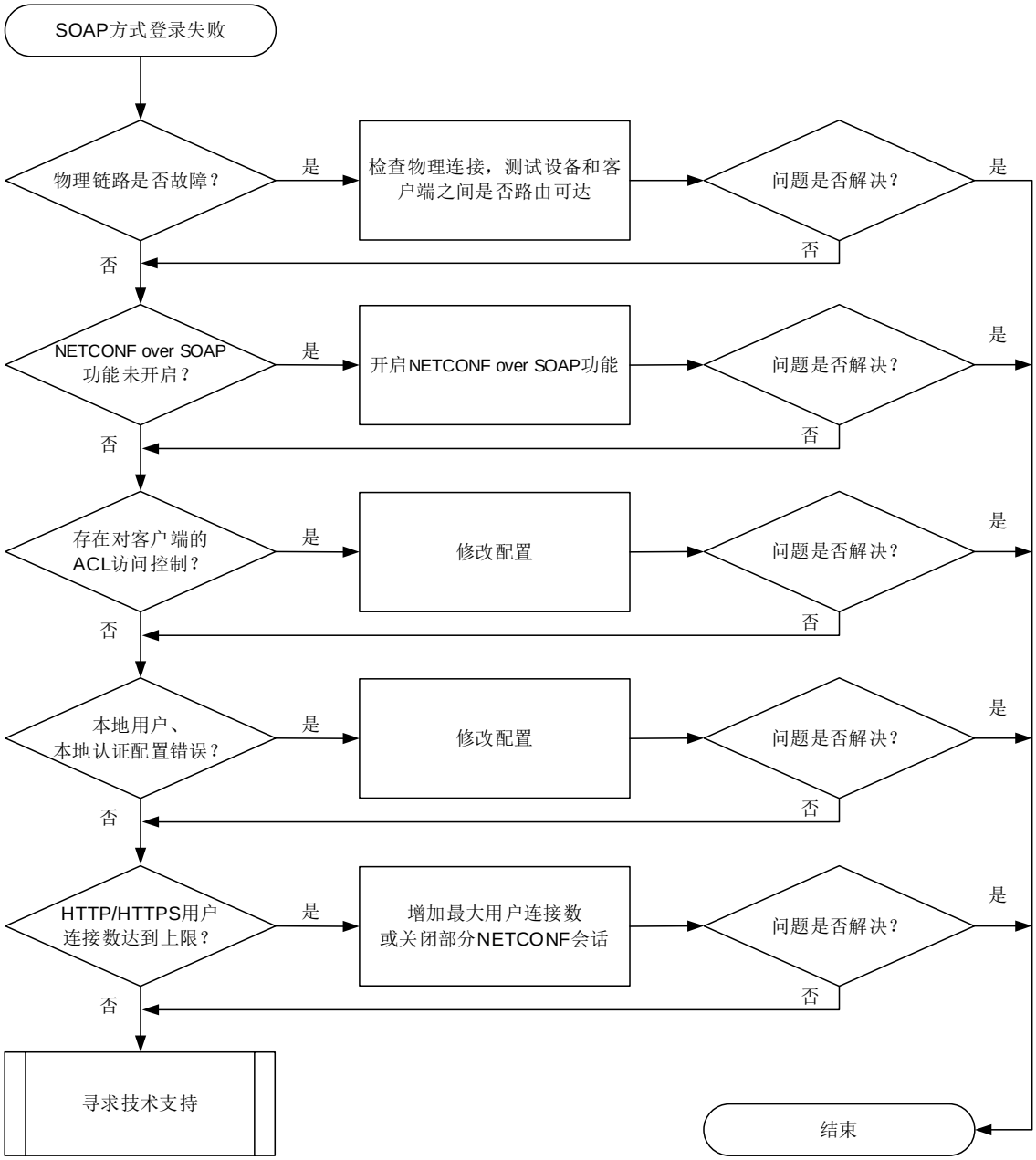
本类故障的常见原因主要包括：

- SOAP 客户端与设备之间路由不通，无法建立 TCP 连接。
- 设备未开启 NETCONF over SOAP 服务器功能。
- 服务器上配置了对客户端的访问控制，但客户端的 IP 地址不在访问控制的 permit 规则内。
- 本地用户未配置授权 HTTP/HTTPS 服务。
- 本地用户认证方式配置不正确。
- HTTP/HTTPS 登录用户数达到允许用户数的上限。

3. 故障分析

本类故障的诊断流程如图 131所示。

图131 SOAP 方式登录失败的故障诊断流程图



4. 处理步骤

(1) 检查物理链路是否存在故障。

可以通过 Telnet 登录设备（用户角色名为 network-admin），在设备上尝试能否 ping 通 NETCONF 客户端的 IP 地址。如果不能 ping 通，在设备上执行 **display ip routing-table** 命令或者 **display route-static routing-table** 命令查看去往客户端的路由出接口，再执行 **display interface** 命令检查该接口状态：

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Interface index: 386
Current state: Administratively DOWN
```

```
Line protocol state: DOWN
...
```

a. 如果 Current state 显示为 Administratively DOWN，则在接口下执行 **undo shutdown** 命令打开关闭的接口。如果 Current state 显示为 DOWN，则检查接口的物理连线是否正确。

b. 如果设备和客户端之间存在其他设备，按上述方法逐跳检查和修复各设备连接的物理接口状态。

(2) 通过 **display netconf service** 命令检查 NETCONF over SOAP 功能是否开启。

```
<Sysname> display netconf service
NETCONF over SOAP over HTTP: Disabled (port 80)
NETCONF over SOAP over HTTPS: Disabled (port 832)
NETCONF over SSH: Disabled (port 830)
NETCONF over Telnet: Enabled
NETCONF over Console: Enabled
...
```

当 NETCONF over SOAP over HTTP 或 NETCONF over SOAP over HTTPS 字段值为 Disabled 时，请在系统视图下执行 **netconf soap http enable**、**netconf soap https enable** 命令开启基于 HTTP/HTTPS 的 NETCONF over SOAP 功能。

(3) 检查是否设置了对客户端 IP 地址的 ACL 访问控制。

```
<Sysname> display current-configuration | begin netconf
 netconf soap http enable
 netconf soap https enable
 netconf soap http acl 2000
#
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] display this
#
acl basic 2000
 rule 5 permit source 192.168.4.10 0
 rule 10 permit source 192.168.4.15 0
...
```

如果存在 **netconf soap { http | https } acl** 命令配置，请按需选择执行以下操作：

- 确保客户端的 IP 地址在相关 ACL 的 **rule** 命令允许的 IP 地址列表中。
- 通过执行 **undo netconf soap { http | https } acl**，使 NETCONF over SOAP 不再关联 ACL。

(4) 使用本地认证时，检查客户端对应的本地用户是否可以使用 HTTP/HTTPS 服务。

进入本地用户视图，执行 **display this** 命令，确保配置了 **service-type http https**。

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-manage-test] display this
#
local-user test class manage
 service-type http https
 authorization-attribute user-role network-operator
```

(5) 使用本地认证时，通过 **display domain** 命令检查用户认证域下的认证、授权、计费配置。

```
<Sysname> display domain
Total 12 domains

Domain: system
  Current state: Active
  State configuration: Active
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
...
```

例如，用户认证域为 system 时，如果缺省的 Authentication、Authorization、Accounting 方案不为 Local，请执行以下命令，将 login 用户的认证、授权、计费方案配置为 Local。

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local
[Sysname-isp-system] authorization login local
[Sysname-isp-system] accounting login local
```

(6) 检查登录到设备的用户数是否达到允许用户数的上限。

在设备上使用 **display netconf service** 命令查看 Active Sessions 字段（当前活跃的 NETCONF 会话数量），如果该字段值已达到 **aaa session-limit** 命令配置的 HTTP/HTTPS 类型的最大用户连接数，请选择以下一种方式进行调整：

- 通过 **aaa session-limit { http | https }** *max-sessions* 命令，配置更大的 HTTP/HTTPS 用户的连接数上限。
- 使用<kill-session>操作，强制释放已建立的部分 SOAP 类型的 NETCONF 会话，使新的用户能够上线。

  # 查看 NETCONF 会话信息的命令如下：

  ```
  <Sysname> display netconf session
  Session ID: 1 Session type : SOAP
    Username : yy
  ...
  ```

  # <kill-session>操作的 XML 报文示例如下：

  ```
  <rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <kill-session>
      <session-id>1</session-id>
    </kill-session>
  </rpc>
  ```

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- NETCONF/6/SOAP_XML_LOGIN

18.1.2 SSH 方式登录失败

1. 故障描述

配置工具通过 SSH 登录设备失败。

2. 处理步骤

请参见“安全类故障处理/SSH 客户端登录设备失败”进行定位。

19 网络管理和监控类故障处理

19.1 Ping和Tracert故障处理

19.1.1 Ping 不通

1. 故障描述

在源端执行 Ping 操作，在一定时间范围内没有收到目的端对该请求的回应。

2. 常见原因

存在三种故障情形：

- 源端没有发出请求报文。
- 目的端没有发出应答报文。
- 中间设备丢包或传输时间长。

本类故障的常见原因主要包括：

- 链路传输时延较长。由于传输时延长，虽然源端接收到了目的端的回应报文，但已经超过等待时限而造成 Ping 不通的现象。
- 配置不当。例如，当 Ping 报文过大时，报文的出接口 MTU 值较小，且设置了不可分片的功能等。
- FIB 表或 ARP 表中缺少对应的表项。
- 存在防攻击配置。
- 硬件故障。

3. 故障分析

本类故障的诊断思路如下：

(1) 检查 Ping 操作是否得当，调整 Ping 操作参数。

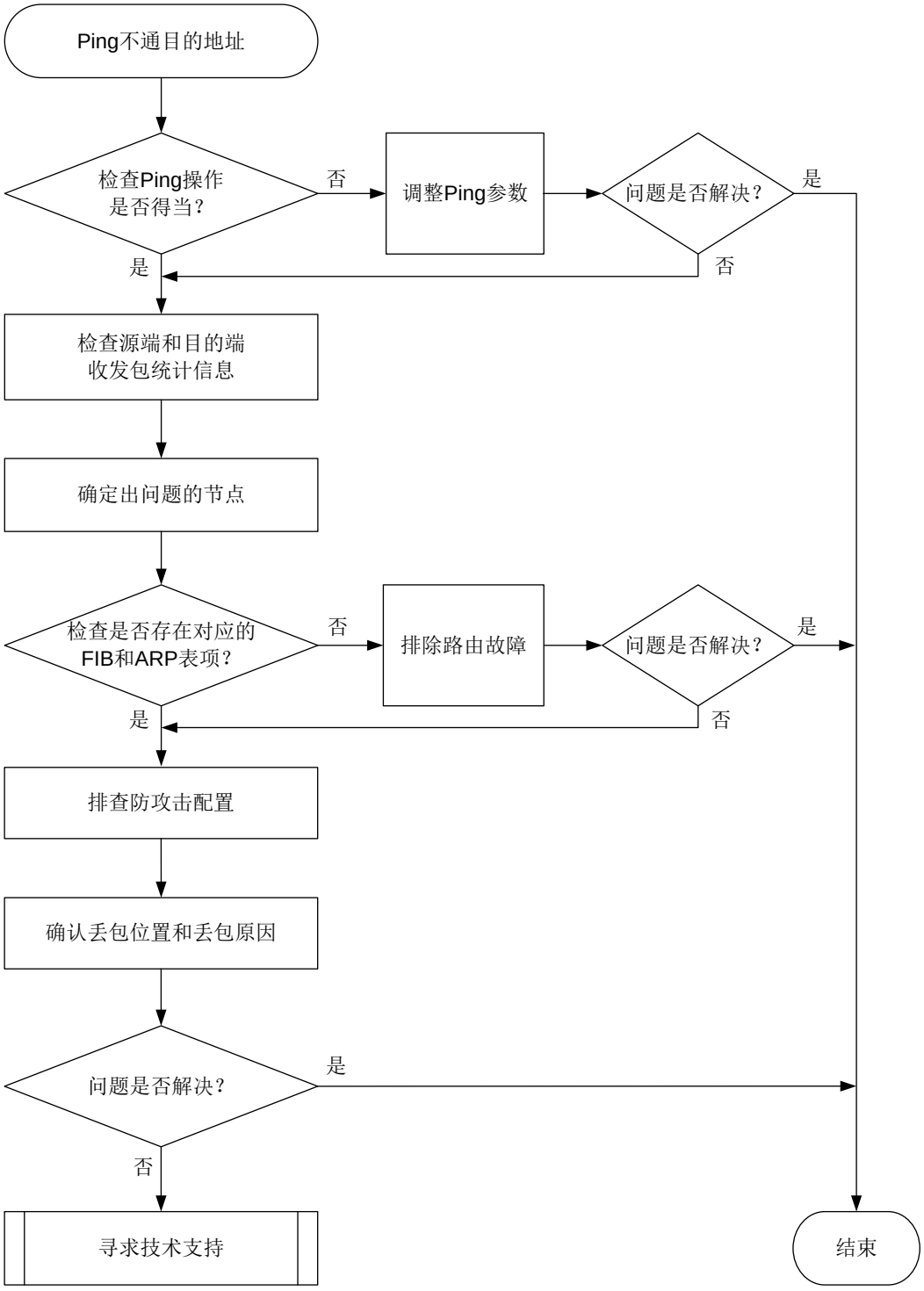
(2) 查看 Ping 报文的统计信息，确认出问题的节点。

(3) 检查是否存在到达目的端的 ARP 以及 FIB 表项。

(4) 排查是否因为防攻击配置导致 Ping 报文被丢弃。

本类故障的诊断流程如图 132 所示。

图132 Ping 不通故障诊断流程图



4. 处理步骤

(1) 检查 Ping 操作是否得当。

a. 检查是否因为实际链路传输时延较长导致 Ping 不通。

检查是否执行了 **ping -t** *timeout* 命令，如果执行了此操作，可通过增加-t 参数的值（建议取值大于等于 1000，达到秒级）或者去掉-t 参数重新 Ping。如果故障消除，则说明较大概率属于实际网络时延大导致的 Ping 不通；如果故障未消除，请继续定位。


说明

-t 参数用来指定 ICMP 回显应答（ECHO-REPLY）报文的超时时间，单位为毫秒，缺省值为 2000。如果源端在 *timeout* 时间内未收到目的端的 ICMP 回显应答（ECHO-REPLY）报文，则会认为目的端不可达。

b. 检查是否因为 Ping 报文过大而被丢弃。

检查是否执行了 **ping -f –s** *packet-size* 命令，如果执行了此操作，且报文转发路径上存在出接口的 MTU 小于报文长度 *packet-size* 的情况，则会导致报文因为超大且不允许被分片而被丢弃。可以通过减小报文长度或者取消**-f** 参数来解决这个问题。


说明

- **-f** 参数表示将长度大于出接口 MTU 的报文直接丢弃，即不允许对发送的 ICMP 回显请求报文进行分片。
- **-s** *packet-size* 参数用来指定发送的 ICMP 回显请求报文的长度（不包括 IP 和 ICMP 报文头），单位为字节，缺省值为 56。

以太网接口 MTU 的缺省值为 1500 字节，可以通过执行 **display interface** 命令来查看接口的 MTU 值：

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
```

其它显示信息略……

c. 检查是否指定了错误的出接口。

检查是否执行了 **ping -i** *interface-type interface-number* 命令指定 Ping 报文的出接口。如果指定了出接口，请确保该接口和目的端之间的物理链路是否可达。否则，请换成其它接口或者去掉-i 参数。


说明

-i *interface-type interface-number* 参数用来指定发送 ICMP 回显请求报文的接口的类型和编号。不指定该参数时，将根据目的 IP 查找路由表或者转发表来确定发送 ICMP 回显请求报文的接口。

d. 检查是否指定了源地址。

检查是否执行了**ping –a** *source-ip* 命令指定Ping报文的源地址。如果执行了该命令，请确保中间设备和目的端有到达源地址 *source-ip* 的路由。


说明

-a *source-ip*：指定ICMP回显请求（ECHO-REQUEST）报文的源IP地址。该地址必须是设备上已配置的IP地址。不指定该参数时，ICMP回显请求报文的源IP地址是该报文出接口的主IP地址。

e. 检查是否为目的端指定了准确的VPN。

根据网络规划和部署情况，确认目的端是否属于某个VPN。如果目的端属于某个VPN，则需要在执行 **ping** 命令时通过**-vpn-instance** 参数指定目的端所属的VPN。

(2) 查看源端、目的端以及中间设备的收发包统计，确认Ping故障发生的方向。

- 检查源端是否发出了ICMP回显请求报文，并收到了ICMP回显应答报文。

  源端执行Ping操作后，在源端和目的端分别使用 **display icmp statistics** 命令查看ICMP报文收发情况。可以根据统计信息中Input和Output区段报文的数量来确定Ping出现问题的方向：

  – 如果源端Output区段的echo值正常增加，但Input区段的echo replies值没有增加，则说明源端发出了请求但是没有收到回应；与此同时，如果目的端Input区段和Output区段的计数都没有变化，则说明目的端没有收到请求也没有给予回应。这样，就可以确定Ping报文是在从源端到目的端的方向上出现了转发故障。

  – 如果源端Output区段的echo值正常增加，但Input区段的echo replies值没有增加，则说明源端发出了请求但是没有收到回应；与此同时，如果目的端Input区段和Output区段的计数都正常增加，则说明目的端收到了请求，同时发出了回应。这样，就可以确定Ping报文是在从目的端到源端的方向上出现了转发故障。

  display icmp statistics 命令显示信息示例如下：

```
<Sysname> display icmp statistics
  Input: bad formats   0                  bad checksum            0
         echo          175                destination unreachable 0
         source quench 0                  redirects               0
         echo replies  201                parameter problem       0
         timestamp     0                  information requests    0
         mask requests 0                  mask replies            0
         time exceeded 0                  invalid type            0
         router advert 0                  router solicit          0
         broadcast/multicast echo requests ignored           0
         broadcast/multicast timestamp requests ignored      0
 Output: echo          0                  destination unreachable 0
         source quench 0                  redirects               0
         echo replies  175                parameter problem       0
         timestamp     0                  information replies     0
         mask requests 0                  mask replies            0
         time exceeded 0                  bad address             0
         packet error  1442               router advert           3
```

其它显示信息略……

提示

- 当目的端是框式设备或者 IRF 设备，且 ICMP 报文到达目的端未被分片时，请在目的端执行带 **slot** 参数的 **display icmp statistics** 命令来查看 ICMP 报文统计信息，**slot** 为目的端接收该 ICMP 报文的接口所在的 Slot。
- 当目的端是框式设备或者 IRF 设备，但 ICMP 报文到达目的端前被分片了，请在目的端执行 **display icmp statistics** 命令来查看 ICMP 报文统计信息即可。

(3) 确定出问题的节点。

确定了 Ping 故障的发生的方向后，请执行 **tracert** 命令确定该方向上报文丢失的位置。

- 如果源端到目的端方向出现了问题，请从源端开始排查。
- 如果目的端到源端方向出现问题，请从目的端开始排查。

如下例所示，可以通过 **tracert** 命令查看报文从源端到目的端（IP 地址为 1.1.3.2，属于 vpn1）所经过的路径，并显示报文经过的私网中的三层设备的信息。

```
<Sysname> tracert –vpn-instance vpn1 –resolve-as vpn 1.1.3.2
traceroute to 1.1.3.2 (1.1.3.2), 30 hops at most, 40 bytes each packet, press CTRL+C
to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms
 3  * * *
```

由以上信息可判断，Ping 报文在 1.1.2.2 的下一跳设备上（即显示为“3 * * *”的节点）出现转发故障。

(4) 检查是否存在到达目的端和源端的 FIB 表项与 ARP 表项。

请在问题节点上执行以下操作：

- 执行 **display fib** 命令检查是否存在到达目的端和源端的路由。如果路由不存在，请检查 OSPF、IS-IS、BGP 等路由协议配置是否有误。
- 如果路由存在并且报文所经链路是以太链路，请执行 **display arp** 命令查看是否存在所需的 ARP 表项。如果 ARP 表项不存在，请首先排查 ARP 故障。

(5) 检查问题节点上是否配置 ICMP 防攻击功能。

如果设备上配置了 ICMP 攻击相关的防范策略，且设备检测到 ICMP 攻击，设备会将 ICMP 报文直接丢弃，从而导致 Ping 不通。

- 通过 **display attack-defense icmp-flood statistics ip** 命令查看统计信息的计数来判断设备是否受到了 ICMP 攻击。
- 通过 **display current-configuration | include icmp-flood**、**display current-configuration | include “signature detect”**查看当前是否配置攻击防范策略。

如果设备受到了 ICMP 攻击，请先定位并解除 ICMP 攻击。

(6) 根据收发包统计，确认丢包位置和丢包原因。

在 Ping 报文途径的设备上：

a. 配置 QoS 策略，使用 ACL 源地址和目的地址过滤 Ping 报文，然后在 Ping 报文途径接口的入方向和出方向应用 QoS 策略。

b. 通过 **display qos policy interface** 命令查看应用 QoS 策略的接口上 QoS 策略匹配成功的报文个数。如果报文个数有增长，则说明设备收到了 Ping 报文；如果报文个数无增长，则说明设备没有收到 Ping 报文，此时，可以使用 **debugging ip packet** 命令打开 IP 报文调试信息开关，进一步排查设备没有收到 Ping 报文的原因并解决问题。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

19.1.2 Tracert 不通

1. 故障描述

执行 Tracert 操作，显示信息中出现“***”行，说明某些节点之间路由不可达，Tracert 不通。

2. 常见原因

本类故障的常见原因主要包括：

- 无对应的路由或者 ARP 表项。
- 中间设备未开启 ICMP 超时报文发送功能。
- 目的端未开启 ICMP 目的不可达报文发送功能。

3. 故障分析

本类故障的诊断思路如下：

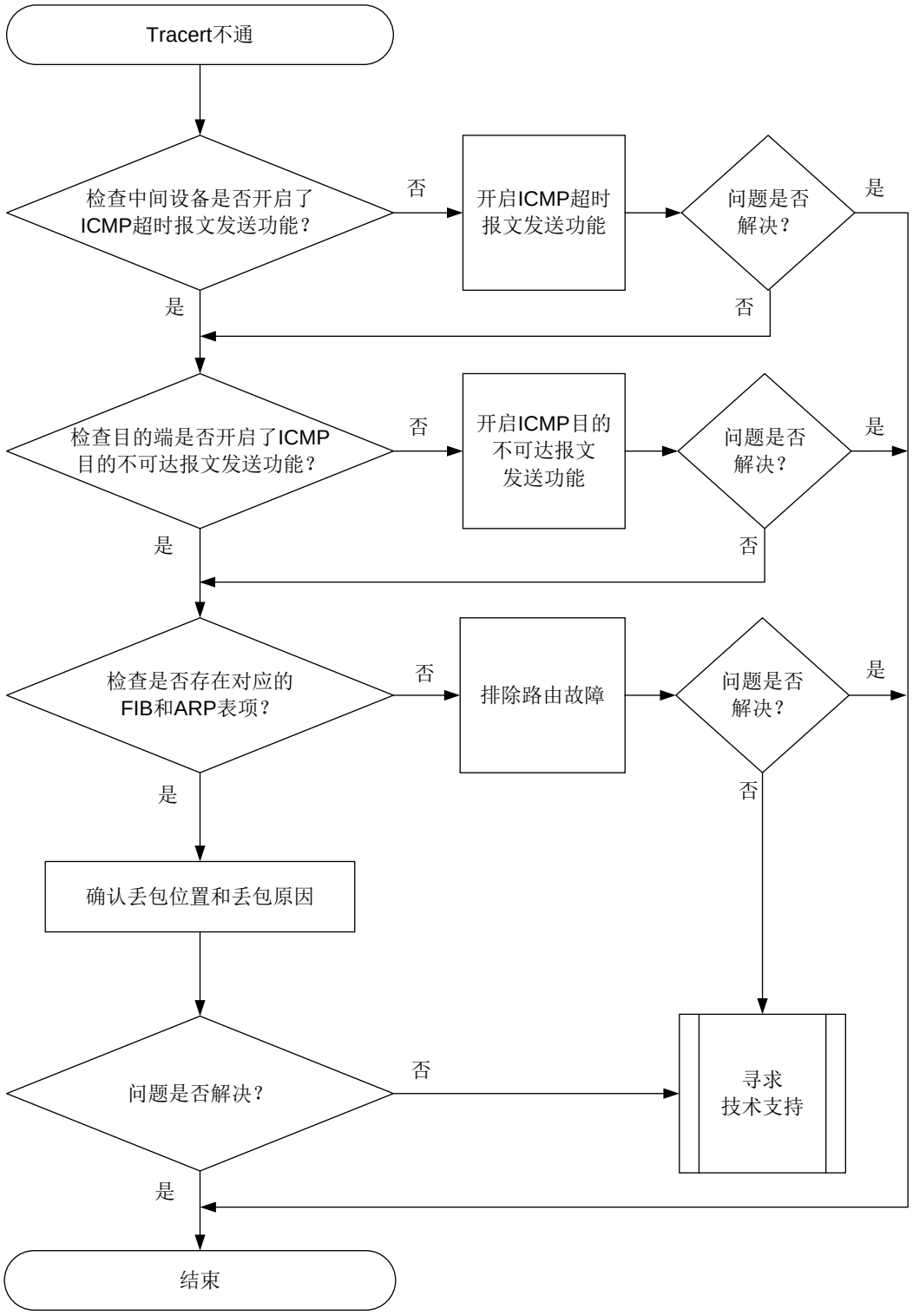
(1) 检查中间设备是否开启了 ICMP 超时报文发送功能。

(2) 检查目的端是否开启了 ICMP 目的不可达报文发送功能。

(3) 检查是否存在达到目的端的 ARP 以及 FIB 表项。

本类故障的诊断流程如图 133 所示。

图133 Tracert 不通故障诊断流程图



4. 处理步骤

(1) 检查中间设备是否开启了 ICMP 超时报文发送功能。

查看报文从源端到目的端所经过的路径（假设源端到目的端只有两跳，目的端的 IP 地址为 1.1.2.2）。

```
<Sysname> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL+C to break
 1 * * *
 2 1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

出现以上显示信息时，请登录中间设备，在中间设备上执行 **ip ttl-expires enable** 命令开启 ICMP 超时报文发送功能。如果故障排除，则说明中间设备未开启 ICMP 超时报文发送功能导致 Tracert 不通；如果故障未排除，请继续执行下面的步骤。

(2) 检查目的端是否开启了 ICMP 目的不可达报文发送功能。

查看报文从源端到目的端所经过的路径（假设源端到目的端只有两跳，目的端的 IP 地址为 1.1.2.2）。

```
<Sysname> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL+C to break
 1 1.1.1.2 (1.1.1.2) [AS 99] 560 ms 430 ms 50 ms
 2 * * *
```

出现以上显示信息时，请在目的端执行 **ip unreachables enable** 命令开启 ICMP 目的不可达报文发送功能。如果故障排除，则说明目的端未开启 ICMP 目的不可达报文发送功能；如果故障未排除，请继续执行下面的步骤。

(3) 在问题节点上检查是否存在对应的 FIB 表项和 ARP 表项。

在未回应 ICMP 差错报文的设备（**tracert** 命令执行结果中显示为“`* * *`”的设备）上执行 **display fib** 命令，检查是否存在到目的地址的路由。

- 如果路由不存在，请检查 OSPF、IS-IS、BGP 等路由协议配置是否有误。
- 如果路由存在并且报文所经链路是以太链路，请执行 **display arp** 命令查看 Tracert 的下一跳地址对应的 ARP 表项是否存在。如果不存在，请检查 ARP 配置是否有误。

(4) 检查 Tracert 发起端是否收到 ICMP 差错报文。

发起 Tracert 后，在 Tracert 发起端上多次执行 **display icmp statistics** 命令查看发起端是否收到 ICMP 差错报文，显示信息示例如下：

```
<Sysname> display icmp statistics
  Input: bad formats   0                   bad checksum            0
         echo          175                 destination unreachable 0
         source quench 0                   redirects               0
         echo replies  201                 parameter problem       0
         timestamp     0                   information requests    0
         mask requests 0                   mask replies            0
         time exceeded 0                   invalid type            0
         router advert 0                   router solicit          0
         broadcast/multicast echo requests ignored           0
         broadcast/multicast timestamp requests ignored      0
```

其它显示信息略……

观察以上 ICMP 报文的统计信息的变化，判断 Input 区段内的 time exceeded 和 destination unreachable 值的增量是否与 Tracert 报文发送个数相等，如果不等则表明发起端未收到 ICMP 差错报文。

(5) 根据收发包统计，确认丢包位置和丢包原因。

在 Tracert 报文途径的设备上：

a. 配置 QoS 策略，使用 ACL 源地址和目的地址过滤 Tracert 报文，然后在 Tracert 报文途径接口的入方向和出方向应用 QoS 策略。

b. 通过 **display qos policy interface** 命令查看应用 QoS 策略的接口上 QoS 策略匹配成功的报文个数。如果报文个数有增长，则说明设备收到了 Tracert 报文；如果报文个数无增长，则说明设备没有收到 Tracert 报文，此时，可以使用 **debugging ip packet** 命令打开 IP 报文调试信息开关，进一步排查设备没有收到 Tracert 报文的原因并解决问题。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

19.2 SNMP故障处理

19.2.1 SNMP 连接失败

1. 故障描述

网管（NMS）通过 SNMP 协议无法成功连接设备。

2. 常见原因

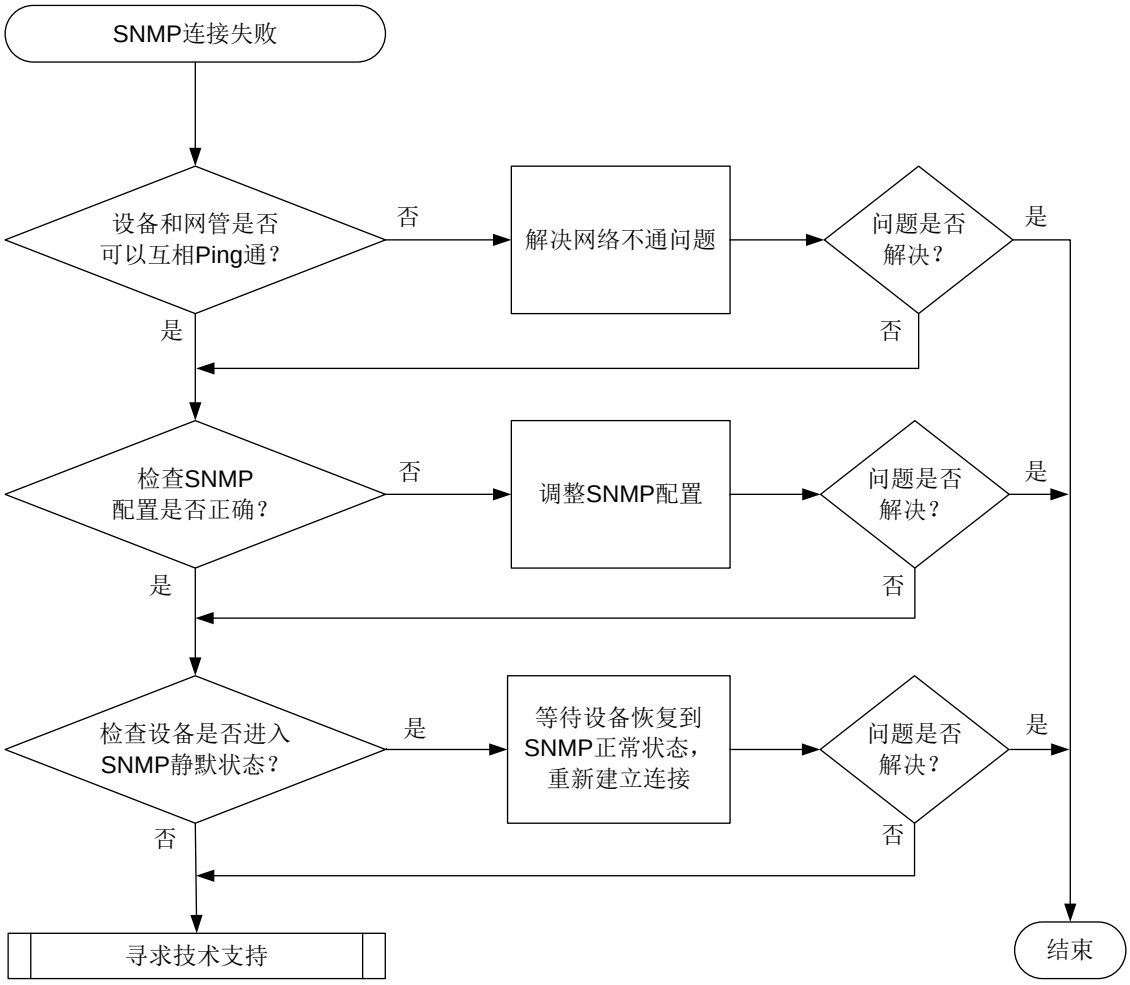
本类故障的常见原因主要包括：

- 网络异常导致报文不可达。
- 配置错误导致认证失败。
- 设备受到 SNMP 报文攻击，进入 SNMP 静默模式。

3. 故障分析

本类故障的诊断流程如图 134 所示。

图134 SNMP 无法连接的故障诊断流程图



4. 处理步骤

(1) 执行 **ping** 命令，检查设备和网管之间是否路由可达。

- 如果可以 Ping 通，说明设备和网管之间路由可达，请执行步骤（2）。
- 如果无法 Ping 通，请参见“Ping 和 Tracert 故障处理”中的“Ping 不通”先解决网络不通问题。待设备和网管之间可以 Ping 通后，重新建立 SNMP 连接。如果重新建立 SNMP 连接后，SNMP 连接仍不能成功建立，请执行步骤（2）。

(2) 检查 SNMP 配置是否正确。

a. 执行 **display snmp-agent sys-info version** 命令，查看设备当前使用的 SNMP 版本号。设备和网管使用的 SNMP 版本号必须相同。如果不同，需使用 **snmp-agent sys-info version** 命令修改配置。

b. 如果当前使用的是 SNMPv1 或 SNMPv2c 版本，则执行 **display snmp-agent community** 命令查看设备上配置的团体信息（包括团体名和使用的 ACL 等信息）。设备和网管使用的团体名必须相同，且设备上配置的 ACL 必须允许网管访问设备。否则，需使用 **snmp-agent community** 和 **acl** 命令修改配置。

c. 如果当前使用的是 SNMPv3 版本，则执行 **display snmp-agent usm-user** 命令查看 SNMPv3 用户信息（包括用户名和使用的 ACL 等信息），并执行 **display snmp-agent**

group 命令查看 SNMP 组信息（包括认证/加密模式和使用的 ACL 等信息）。设备和网管使用的用户名必须相同，认证/加密参数必须一致，且设备上配置的 ACL 必须允许网管访问设备。否则，需使用 **snmp-agent group**、**snmp-agent usm-user v3** 和 **acl** 命令修改配置。

(3) 检查设备是否进入 SNMP 静默状态。

如果 1 个统计周期内（时长为 1 分钟）设备收到的 SNMP 认证失败报文的个数大于等于 100，则设备认为受到了 SNMP 攻击，SNMP 模块会进入静默状态（设备会打印日志 SNMP agent is now silent），设备将在 4～5 分钟内不再响应收到的任何 SNMP 报文。请等待 SNMP 静默状态解除后，重新建立 SNMP 连接。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：SNMPv2-MIB

- authenticationFailure (1.3.6.1.6.3.1.1.5.5)

相关日志

- SNMP/3/SNMP_ACL_RESTRICTION
- SNMP/4/SNMP_AUTHENTICATION_FAILURE
- SNMP/4/SNMP_IPLOCK
- SNMP/4/SNMP_IPLOCKSTAT
- SNMP/4/SNMP_SILENT
- SNMP/5/SNMP_IPUNLOCK
- SNMP/5/SNMP_IPUNLOCKSTAT

19.2.2 SNMP 操作超时

1. 故障描述

网管（NMS）对设备执行 SNMP Get 和 Set 操作，网管侧提示操作超时，导致操作失败。

2. 常见原因

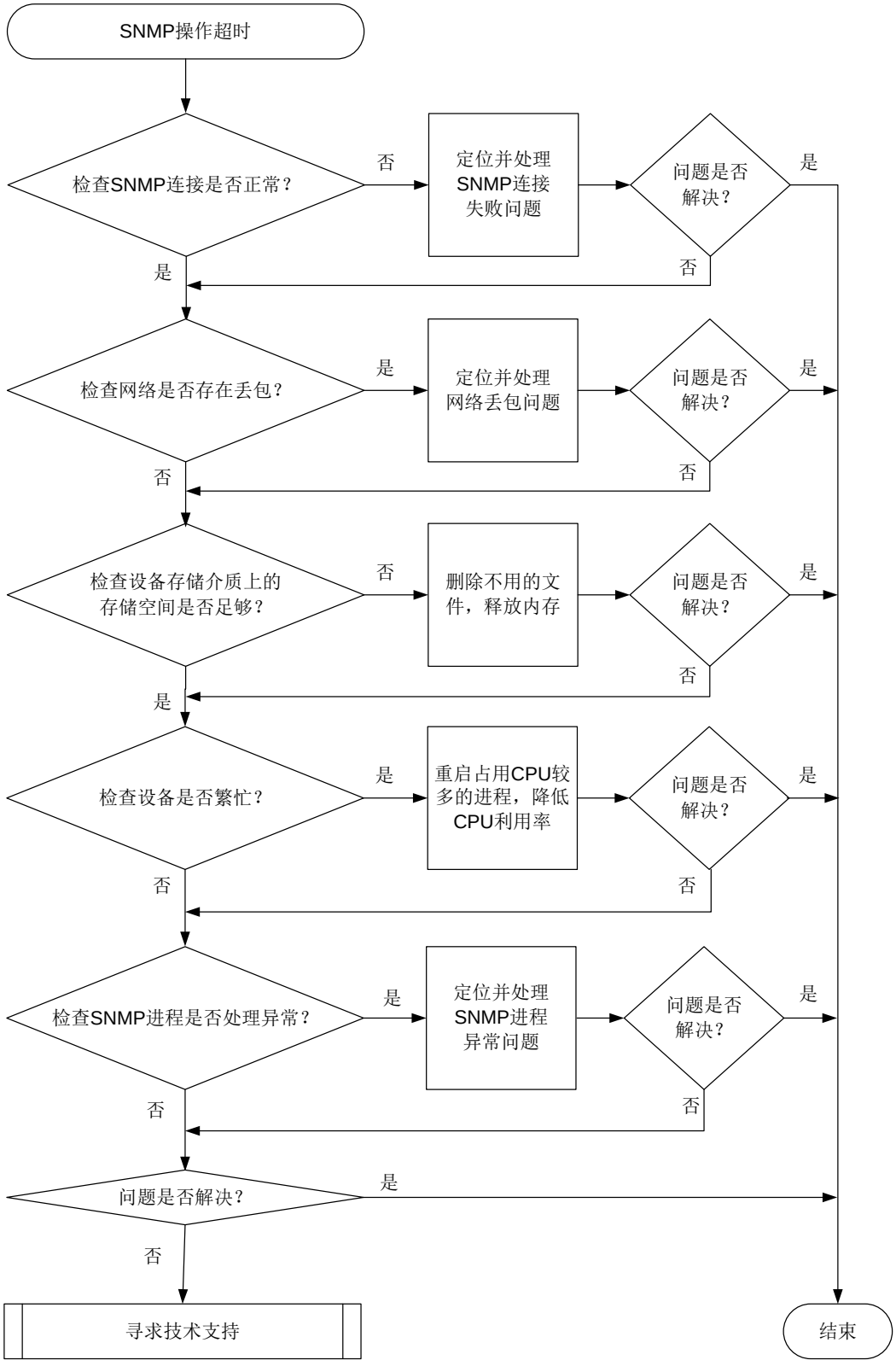
本类故障的常见原因主要包括：

- SNMP 连接中断，导致网管无法访问设备。
- 网络丢包，导致设备没有收到 SNMP 请求。
- 设备存储介质上的存储空间不足，导致设备无法处理 SNMP 请求。
- 设备繁忙，正在处理其它业务，导致无法处理 SNMP 请求。
- SNMP（作为 SNMP agent）进程忙，正在处理其它 SNMP 请求，导致无法对当前 SNMP 请求做出应答。
- SNMP 进程处理当前 SNMP 请求时发生异常。

3. 故障分析

本类故障的诊断流程如图 135 所示。

图135 SNMP 操作超时的故障诊断流程图



4. 处理步骤

(1) 定位并处理 SNMP 连接问题。

在网管上查看 SNMP 连接，如果显示连接超时或者失败，请参照“SNMP 连接失败”故障处理章节先定位并处理 SNMP 连接问题。

(2) 检查网络是否存在丢包。

在网管设备上使用 **ping -c** *count host* 命令，例如将 *conut* 参数设置为 100，*host* 参数取值为设备的 IP 地址，查看 **ping** 命令执行结果中的 packet loss 字段取值，判断网络是否存在丢包。

- 如果无丢包，请参照步骤（3）继续定位；
- 如果有丢包，请参见“Ping 和 Tracert 故障处理”中的“Ping 不通”先解决网络不通问题。

说明

-c *count*：指定 ICMP 回显请求报文的发送次数，取值范围为 1～4294967295，缺省值为 5。

(3) 定位并处理设备存储介质上的存储空间不足问题。

在任意视图下执行 **display memory-threshold** 命令，如果显示信息中的“Current free-memory state”字段取值中包含 Normal 字样，表示设备存储介质上的存储空间充足，否则，表示设备存储介质上的存储空间不足，请使用以下方法清理内存。

- 使用 **reset recycle-bin** 命令清除回收站中的文件。（回收站中的文件也会占用存储介质上的存储空间。）
- 使用 **delete /unreserved** *file* 命令一次性彻底删除文件。如果未使用**/unreserved** 参数，删除的文件会保存在回收站中。

说明

根据设备型号不同，设备支持的存储介质可能为 Flash、CF 卡等。

(4) 定位并处理设备繁忙问题。

a. 在任意视图下多次重复执行 **display cpu-usage** 命令，查看设备 CPU 利用率是否持续在较高水平。

b. 在任意视图下执行 **monitor process** 命令，检查是否存在占用较多 CPU 的进程。如果某个业务进程占用 CPU 较多，可以根据业务需要以及设备支持情况，通过重启服务来降低 CPU 利用率。

(5) 定位 SNMP 进程问题。

对于支持 **display system internal snmp-agent operation in-progress** 命令的设备，在系统视图下执行 **probe** 命令，进入 Probe 视图，然后多次重复执行 **display system internal snmp-agent operation in-progress** 命令查看设备正在处理的 SNMP 操作的相关信息。

- 如果显示信息中的 Request ID 取值一直在变化，则说明 SNMP 进程一直在处理不同的请求，当前 SNMP 进程业务较忙。请降低网管对设备的 SNMP 操作频率。

- 如果显示信息中的 Request ID 取值一直不变，则说明 SNMP 进程一直在处理同一请求，SNMP 进程处理该请求时超时。可通过以下方法排除故障：
  - 依次执行 **undo snmp-agent** 命令和 **snmp-agent** 命令重启 SNMP 进程，来尝试排除故障。
  - 执行 **display system internal snmp-agent operation timed-out** 和 **display system internal snmp-agent packet timed-out** 命令确认耗时较多的 SNMP 操作以及该操作涉及的 MIB 节点，减少或不要执行类似操作。

(6) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无

19.2.3 网管无法管理设备

1. 故障描述

网管对设备执行 SNMP Set 或 Get 等操作，设备无响应或者提示操作失败。

2. 常见原因

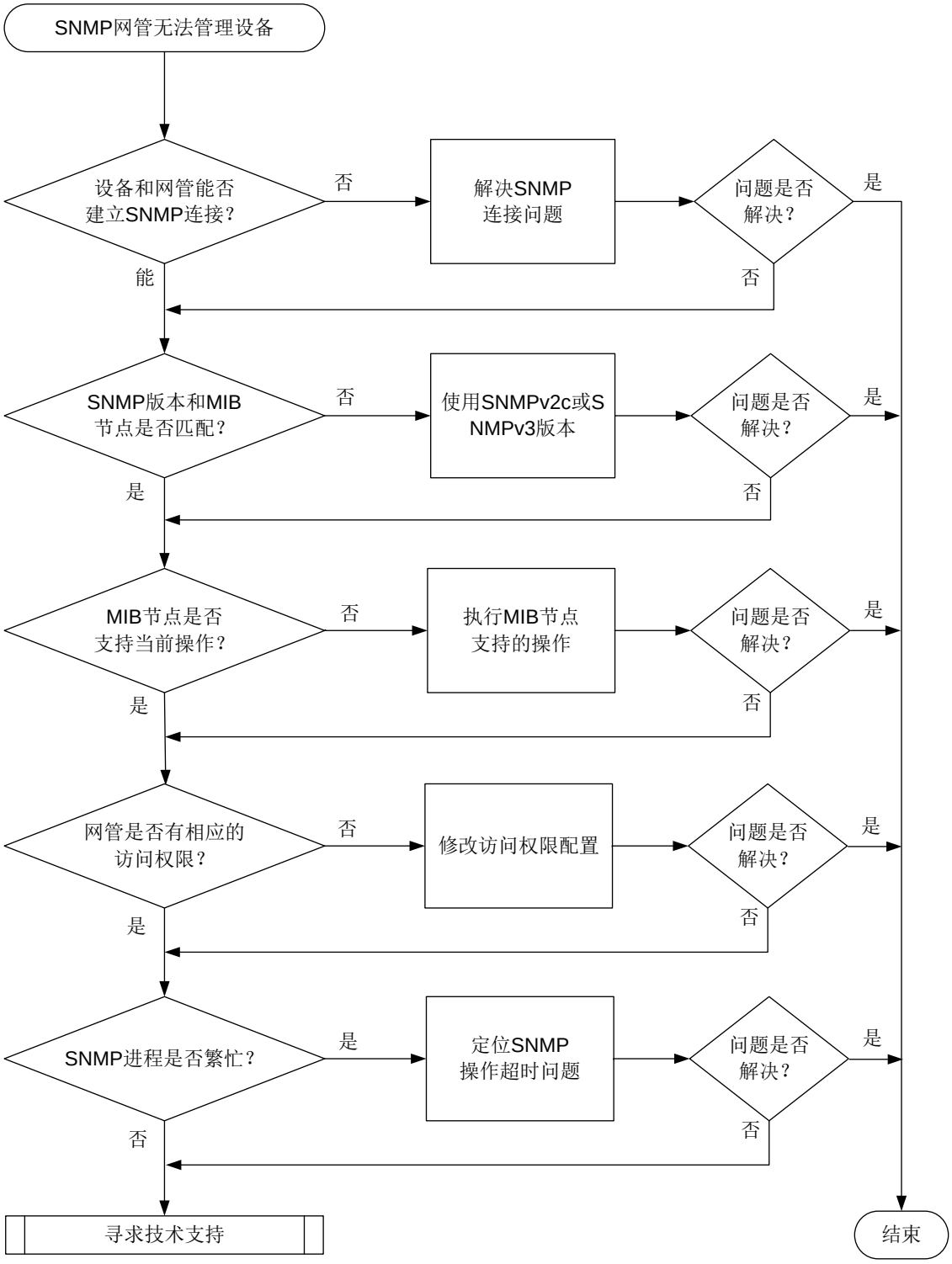
本类故障的常见原因主要包括：

- 网管通过 SNMP 协议无法成功连接设备。
- 网管使用的 SNMP 版本和 MIB 节点不匹配。
- 网管没有访问设备的权限。
- 设备上的 SNMP 进程忙，无法对当前 SNMP 请求做出应答。

3. 故障分析

本类故障的诊断流程如图 136所示。

图136 网管无法管理设备的故障诊断流程图



4. 处理步骤

(1) 检查网管是否可以通过 SNMP 协议连接设备。

如果网管通过 SNMP 协议无法成功连接设备，请参照 SNMP 连接失败故障处理流程进行处理。

(2) 检查网管当前使用的 SNMP 协议版本是否支持访问该 MIB 节点。

例如 snmpUsmMIB 只支持通过 SNMPv3 协议访问；Integer32、Unsigned32 和 Counter64 数据类型仅 SNMPv2c 和 SNMPv3 版本支持。如果网管使用 SNMPv1 版本和设备相连，网管将无法访问 Integer32、Unsigned32 和 Counter64 数据类型的 MIB 节点。MIB 节点的数据类型可通过 MIB 文件中节点的 SYNTAX 字段查看。

```
hh3cDhcpServer2BadNum OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of the bad packets received."
    ::= { hh3cDhcpServer2StatGroup 1 }
```

如果因为版本原因导致网管无法访问 MIB 节点，请将网管切换到 SNMPv2c 或 SNMPv3 版本后，与设备重新建立连接，再执行 Get 和 Set 操作。

(3) 检查 MIB 节点是否支持当前的访问操作。

请根据 MIB 节点支持的操作类型来访问设备。MIB 节点支持的操作类型可通过 MIB 文件中节点的 MAX-ACCESS 字段查看。

```
hh3cDhcpServer2BadNum OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of the bad packets received."
    ::= { hh3cDhcpServer2StatGroup 1 }
```

(4) 检查网管的访问权限。如果访问权限不够，请在设备上修改对应配置，给网管授权。

SNMP 支持的访问控制方式包括：

- VACM（View-based Access Control Model，基于视图的访问控制模型）：将团体名/用户名与指定的 MIB 视图进行绑定，可以限制 NMS 能够访问哪些 MIB 对象，以及对 MIB 对象不同的操作权限。通过 **display current-configuration | include view** 命令可查看 MIB 视图相关配置，通过 **display snmp-agent mib-view** 命令可查看 MIB 视图的详细信息。如果配置错误，请修改 MIB 的相关配置。

  设备支持三种 MIB 视图：

  - Read-view：网管只能读取该视图中节点的值。
  - Write-view：网管可读和写该视图中节点的值。
  - Notify-view：当该视图中包含的 Trap 节点到达触发条件，网管会收到对应的 Trap/Inform 报文。

- RBAC（Role Based Access Control，基于角色的访问控制）：我司设备通过 RBAC 进行用户访问权限控制。RBAC 的基本思想就是给用户指定角色，这些角色中定义了允许用户操作哪些系统功能以及资源对象。创建 SNMPv3 用户名时，可以绑定对应的用户角色，通过用户角色下制定的规则，来限制 NMS 能够访问哪些 MIB 对象，以及对 MIB 对象不同的操作权限。如果 RBAC 权限配置错误，可以通过 **role name** 命令进入用户角色视图修改用户角色的规则。

– 拥有 network-admin 或 level-15 用户角色的 SNMP 团体/用户，可以对所有的 MIB 对象进行读写操作；
– 拥有 network-operator 用户角色的 SNMP 团体/用户，可以对所有的 MIB 对象进行读操作；
– 拥有自定义用户角色的 SNMP 团体/用户，可以对角色规则中指定的 MIB 对象进行操作。


说明

为了安全起见，只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才能配置 SNMP 团体、用户或组。请确保登录用户具有 network-admin 或者 level-15 用户角色，以免配置失败。

(5) 检查 SNMP 进程是否繁忙。

网管对设备执行 SNMP Set 或 Get 等操作，设备无响应或者提示操作失败，还可能因为 SNMP 进程忙，无法对当前 SNMP 请求做出应答，请参照 SNMP 操作超时故障处理流程进行处理。

(6) 其它建议

建议网管通过业务接口访问设备，因为业务接口的报文处理能力优于网管口，以便 SNMP 报文能尽快得到处理。

当有多个 NMS 同时访问设备，且设备反应缓慢时，建议降低访问频率来减轻设备分担，例如将访问频率设置成大于等于 5 分钟。

(7) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

模块名：SNMPv2-MIB

- authenticationFailure (1.3.6.1.6.3.1.1.5.5)

相关日志

- SNMP/3/SNMP_ACL_RESTRICTION
- SNMP/4/SNMP_AUTHENTICATION_FAILURE
- SNMP/4/SNMP_IPLOCK
- SNMP/4/SNMP_IPLOCKSTAT
- SNMP/4/SNMP_SILENT
- SNMP/5/SNMP_IPUNLOCK
- SNMP/5/SNMP_IPUNLOCKSTAT

19.2.4 网管无法收到设备发送的 Trap

1. 故障描述

网管无法收到设备发送的 Trap 报文。

2. 常见原因

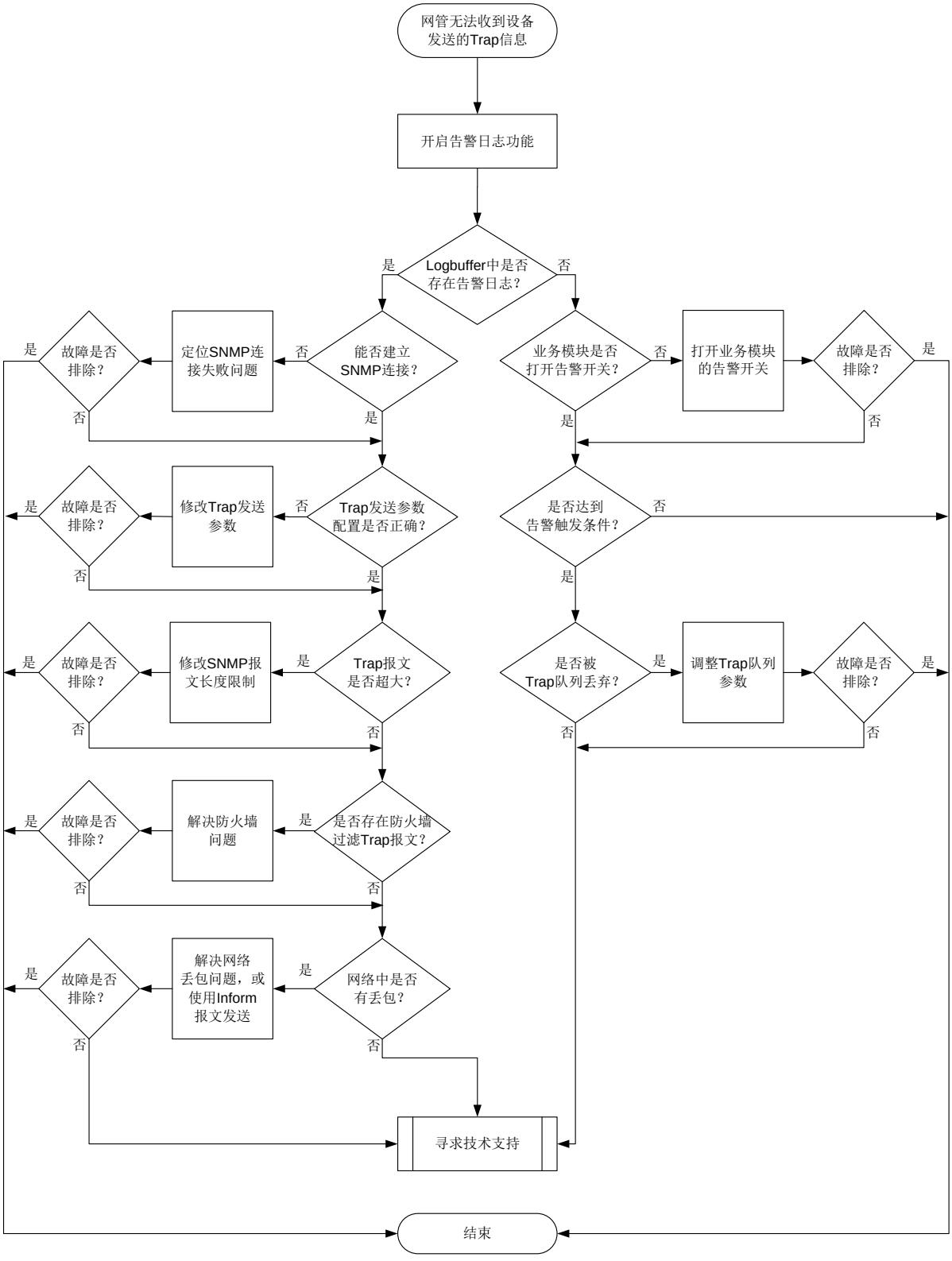
本类故障的常见原因主要包括：

- 设备和网管之间路由不可达，或者 SNMP 功能异常，导致无法建立 SNMP 连接。
- 设备侧和网管侧配置错误，导致网管无法收到设备发送的告警。
- 设备侧业务模块没有产生告警。
- 告警报文丢失，导致网管未收到设备发送的告警。
- SNMP Trap 报文过大，超过 SNMP 模块对 Trap 报文大小的限制。

3. 故障分析

本类故障的诊断流程如图 137 所示。

图137 网管无法收到设备发送的 Trap 的故障诊断流程图



4. 处理步骤

(1) 在系统视图下通过 **snmp-agent trap log** 命令开启 SNMP 告警日志功能。当设备向网管发送告警时，会同时在设备上生成一条日志来记录该 Trap。

(2) 通过 **display logbuffer | include SNMP_NOTIFY** 命令可以查看设备上是否生成 Trap 以及生成的 Trap 详情。

- 如果有显示信息，说明设备有 Trap 生成。请执行步骤(3)。
- 如果没有显示信息，说明 SNMP 模块未向外发送 Trap。请执行步骤(4)。

(3) 如果设备生成了 Trap，但网管未收到 Trap，请参照以下步骤定位。

a. 检查设备是否可以和网管建立 SNMP 连接。如果连接建立失败，请参见 SNMP 连接失败故障处理流程解决 SNMP 连接建立失败问题。

b. 通过 **display current-configuration | include snmp** 命令查看 **snmp-agent target-host trap** 命令配置是否正确。如果不正确，请修改配置，保证指定的 IP 地址（VPN 参数）和端口号与网管用来接收 Trap 报文的 IP 地址（网管所属 VPN）和端口号一致，以及设备和网管使用的 SNMP 协议、安全字一致。

- 如果使用 SNMPv1 或 SNMPv2c 版本，则安全字为团体名，请在设备上使用 **snmp-agent community** 命令创建 SNMP 团体。
- 如果使用 SNMPv3 版本，则安全字为用户名，且设备和网管使用的认证和加密级别必须相同。您需要在设备上使用 **snmp-agent group** 和 **snmp-agent usm-user v3** 命令创建 SNMPv3 用户，创建用户时配置的认证和加密模式、认证密码和加密密码（如果用到）必须和网管侧一致，且创建用户时配置的认证和加密级别必须比 **snmp-agent target-host trap** 命令中指定的认证和加密级别高。安全级别分为：不认证不加密、认证不加密和认证加密，安全级别依次升高。
- 团体名和用户名可访问的 MIB view 必须包含对应的 MIB 告警节点，否则，会因为权限问题导致设备不会将 Trap 报文发送给网管。

c. 执行 **debugging udp packet** 命令打开 UDP 报文的调试信息开关，查看设备发送的 Trap 报文是否过大。如果业务模块封装的数据较多，可能会导致 Trap 报文大于设备能发送的 SNMP 报文的最大长度，这样的 Trap 报文会被丢弃。此时可结合网络的 MTU 值以及是否支持分片情况，通过 **snmp-agent packet max-size** 命令修改设备能发送的 SNMP 报文的最大长度。

```
*Dec 27 22:35:41:203 2021 Sysname SOCKET/7/UDP: -MDC=1;
UDP Output:
 UDP Packet: vrf = 0, src = 192.168.56.121/30912, dst = 192.168.56.1/162
             len = 79, checksum = 0xd98f
```

d. 检查网络中是否存在防火墙过滤 Trap 报文。

如果网络中设置了防火墙，可采用以下措施来解决问题：

- 如果防火墙对报文的源 IP 进行了过滤，可使用 **snmp-agent trap source** 命令修改 Trap 报文的源 IP 地址。
- 修改防火墙的规则，放行 Trap 报文。

e. 检查网络是否不稳定，存在丢包。

如果网络中存在丢包，可采用以下措施来解决问题：

- 检查网络，解决网络丢包问题。

– 配置使用 Inform 报文发送告警信息。Inform 有确认机制，比 Trap 更可靠。Inform 仅 SNMPv2c 和 SNMPv3 支持。

(4) SNMP 模块未向外发送 Trap，请参照以下步骤定位。

a. 通过 **display snmp-agent trap-list** 查看业务模块的告警功能是否开启。如未开启，可通过 **snmp-agent trap enable** 命令开启。

b. 检查是否达到告警条件。例如接口状态告警会在接口状态发生变化时产生，CPU 和内存告警会在 CPU、内存的利用率超过阈值时产生等。

– 如未达到告警条件，未产生 Trap，属正常现象，无需处理。

– 如果达到告警条件，设备未向外发送 Trap，请执行步骤(c)。

c. 使用 **display snmp-agent trap queue** 命令查看 Trap 缓冲区是否被占满。如果 Message number 大于 Queue size，表示 Trap 缓冲区可能被占满，新生成的 Trap 报文可能被丢弃。此时，可在系统视图下使用 **snmp-agent trap queue-size** 和 **snmp-agent trap life** 命令来调整 Trap 缓冲区性能参数。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- SNMP/6/SNMP_NOTIFY
- SNMP/3/SNMP_INFORM_LOST

19.3 镜像故障处理

19.3.1 配置流镜像后监控设备收不到镜像报文

1. 故障描述

配置流镜像后，监控设备收不到镜像报文。

2. 常见原因

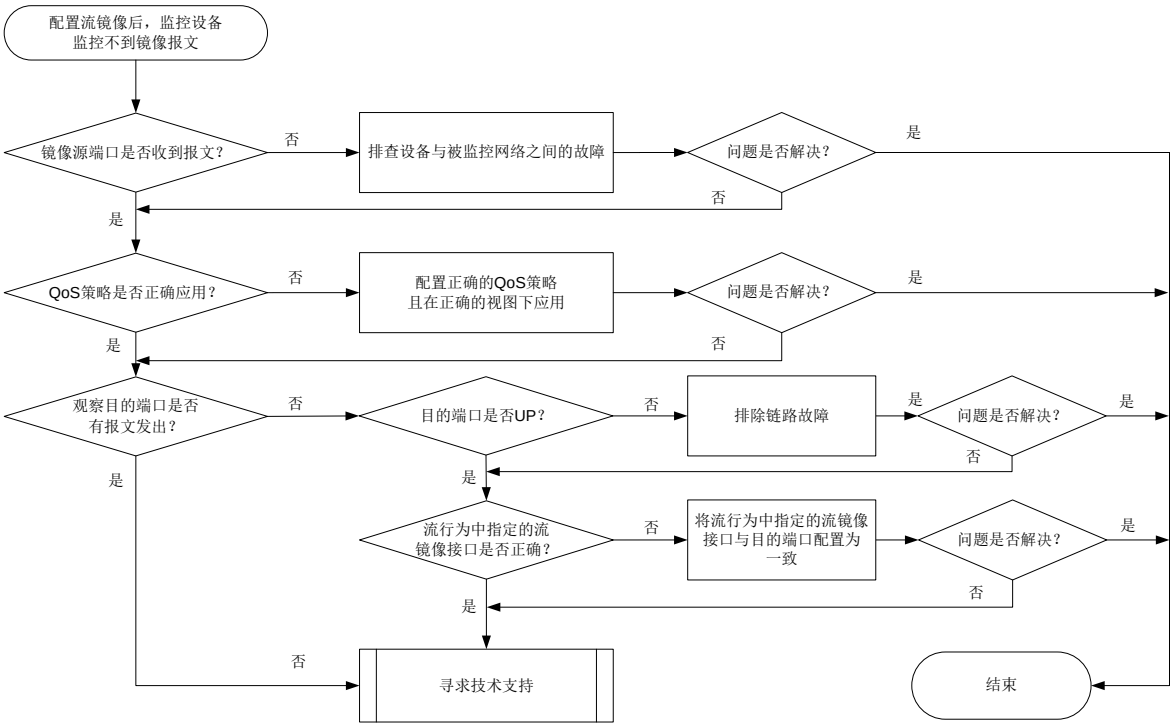
本类故障的常见原因主要包括：

- 目的接口与被监控网络间链路存在故障。
- QoS策略未被应用或者报文未匹配QoS策略。
- 配置流行为时，指定的流镜像接口错误。

3. 故障分析

本类故障的诊断流程如 12.3.1 3. 图 87 所示。

图138 配置流镜像后监控设备收不到镜像报文的故障诊断流程图



4. 处理步骤

(1) 检查镜像源端口能否成功收发报文。

在源设备上执行 **display interface** *interface-type interface-number* 命令，通过显示信息中的“Input(total)”、“Output(total)”字段查看端口收发报文的统计值。

- 如果镜像源端口收发的报文的统计信息为 0 或者不变化，此时设备与被监控的网络之间可能存在链路故障（比如端口 Down 等），请排查解决。
- 如果镜像源端口收发的报文的统计信息不为 0 且不断变化，请执行步骤(2)。

(2) 检查 QoS 策略是否被正确应用。

排查匹配待镜像报文的 QoS 策略是否被应用以及应用的 QoS 策略是否正确。

在源设备上执行 **display qos policy interface** 命令检查镜像源端口上是否应用 QoS 策略。

- 如果未应用，请根据实际组网需要，在镜像源端口上应用 QoS 策略。
- 如果已应用，继续检查 QoS 策略配置是否正确。在设备上执行 **display qos policy** 命令检查 QoS 策略的配置信息。显示信息中 Classifier 字段和 Behavior 字段分别对应配置的流分类和流行为。
  - 如果引用的错误，则在系统视图下执行 **qos policy** 命令进入对应的 QoS 策略视图，执行 **classifier behavior** 命令来修改 QoS 策略引用的流分类和流行为。QoS 策略的具体的定位修改，请参见“MQC 方式配置的 QoS 策略未生效”。
  - 如果引用正确，请执行步骤(3)。

(3) 检查目的端口是否有报文发出。

在目的设备上执行 **display interface** *interface-type interface-number* 命令，通过显示信息中的“Output(total)”字段查看端口发送的报文的统计值。

- 如果目的端口发出的报文的统计信息为 0 或者不变化。在设备上执行 **display interface** *interface-type interface-number* 命令查看显示信息中的“Current state”字段，确认接口的物理状态是否为 Up。
  - 如果为 Up，请执行步骤。
  - 如果为 Down，请排查处理接口物理 Down 的问题。
- 如果目的端口发出的报文的统计信息不为 0 且不断变化，请执行步骤(8)。

(4) 检查在目的端口上应用的 QoS 策略中，流行为视图下配置的流镜像接口（通过 **mirror-to interface** 命令配置）是否为目的端口。

- 如果不是，请通过 **mirror-to interface** 命令将流镜像接口重新配置为正确的接口。
- 如果是，请执行步骤(8)。

(5) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

- QOS_POLICY_APPLYIF_CBFAIL
- QOS_POLICY_APPLYIF_FAIL
- QOS_POLICY_APPLYGLOBAL_CBFAIL
- QOS_POLICY_APPLYGLOBAL_FAIL

19.3.2 配置端口镜像后监控设备收不到镜像报文

1. 故障描述

配置流镜像后，监控设备收不到镜像报文。

2. 常见原因

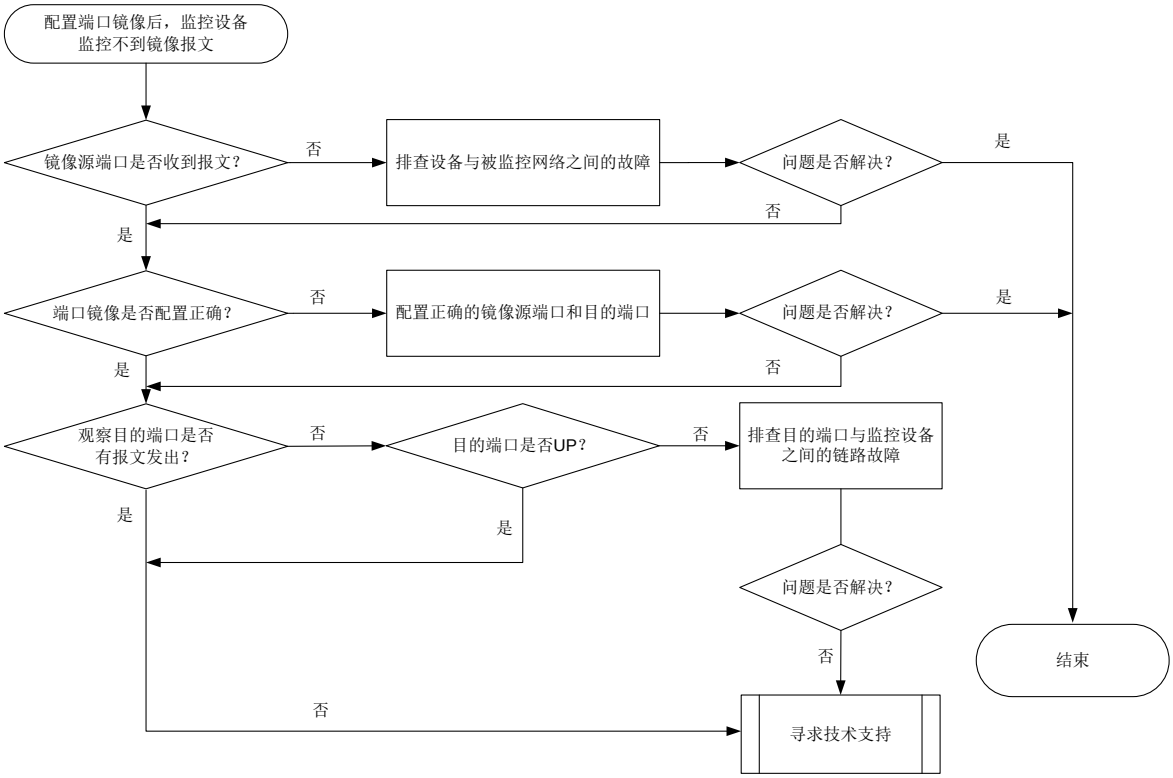
本类故障的常见原因主要包括：

- 镜像源接口与被监控网络间链路存在故障。
- 镜像源端口或镜像目的端口配置错误。

3. 故障分析

本类故障的诊断流程如图 139 所示。

图139 端口镜像后监控设备收不到镜像报文的故障诊断流程图



4. 处理步骤

(1) 检查镜像源端口能否成功收发报文。

在源设备上执行 **display interface** *interface-type interface-number* 命令，通过显示信息中的“Input(total)”、“Output(total)”字段查看端口收发报文的统计值。

- 如果镜像源端口收发的报文的统计信息为 0 或者不变化，此时设备与被监控的网络之间可能存在链路故障（比如端口 Down 等），请排查解决。
- 如果镜像源端口收发的报文的统计信息不为 0 且不断变化，请执行步骤(2)。

(2) 检查端口镜像配置是否正确。

在源设备上执行 **display mirroring-group** 命令检查端口镜像的配置信息，确认配置的镜像源端口和镜像目的端口是否正确。其中，显示信息中“Mirroring port”字段为镜像源端口、“Monitor port”字段为镜像目的端口。

- 如果正确，请执行步骤(3)。
- 如果不正确，请在系统视图下分别执行 **mirroring-group mirroring-port** 和 **mirroring-group monitor-port** 命令重新将镜像源端口和镜像目的端口配置正确。

(3) 检查目的端口是否有报文发出。

在目的设备上执行 **display interface** *interface-type interface-number* 命令，查看显示信息中的“Output(total)”字段查看端口发送的报文的统计值。

- 如果目的端口发出的报文的统计信息为 0 或者不变化。在设备上执行 **display interface** *interface-type interface-number* 命令查看显示信息中的“Current state”字段，确认接口的物理状态是否为 Up。

- 如果为 Up，请执行步骤。
- 如果为 Down，请排查处理接口物理 Down 的问题。

- 如果目的端口发出的报文的统计信息不为 0 且不断变化，请执行步骤(4)。

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

无

20 网络管理类故障处理

20.1 gRPC故障处理

20.1.1 gRPC 采样周期不准确

1. 故障描述

gRPC Dial-out 模式向采集器上送的订阅报文中，某些数据源的采样周期与用户配置的采样周期不一致。

2. 常见原因

本类故障的常见原因主要包括：

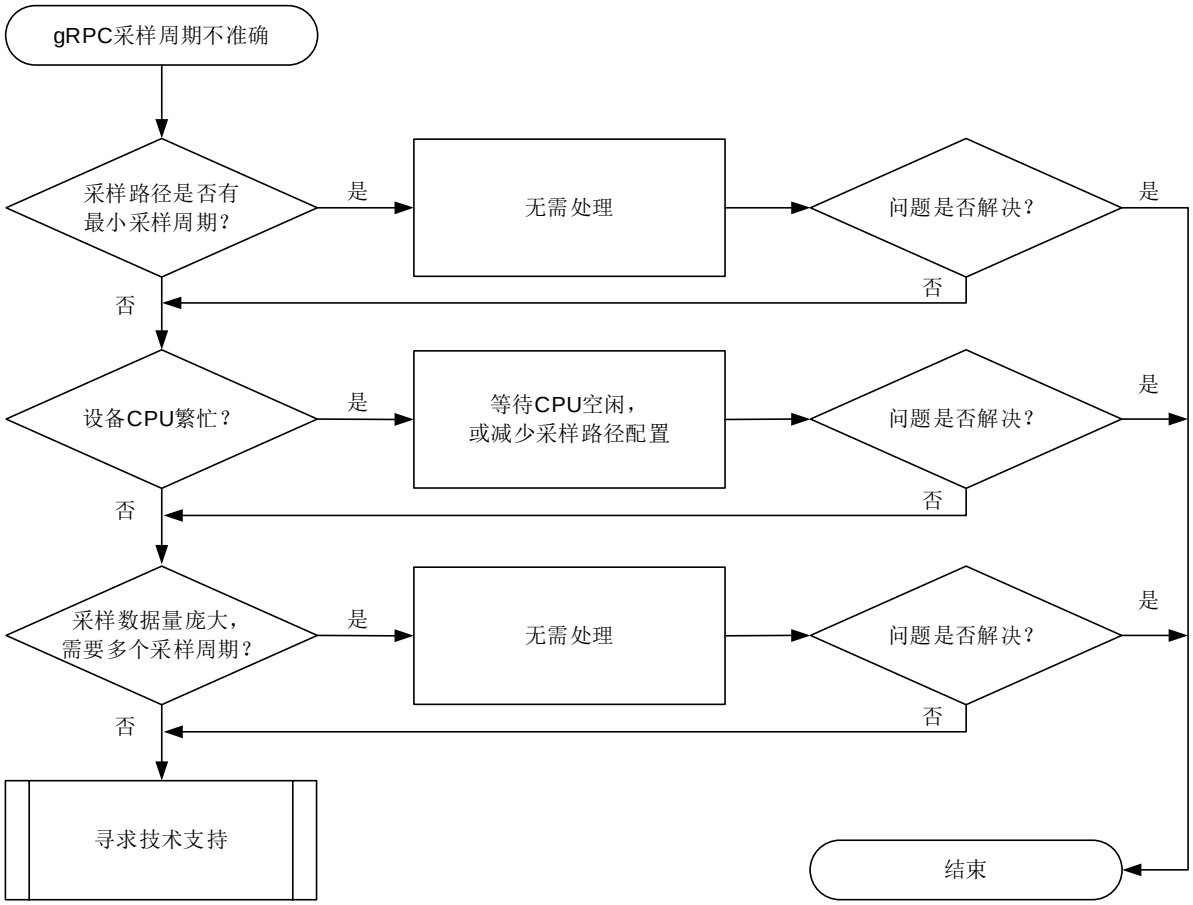
- 部分采样路径无法达到配置的采样周期精度，以自身的最小采样周期进行采样。
- 设备 CPU 繁忙。
- 数据源对应的采样路径为 ifmgr/interfaces、路由类或统计类路径，由于采样数据量庞大，需要使用多个采样周期。

  例如 route/ipv4routes，当路由表项达到 100k 时，采样数据量大，设备无法在一个较小的采样周期完成采集工作。

3. 故障分析

本类故障的诊断流程如图 140 所示。

图140 gRPC 采样周期不准确的故障诊断流程图



4. 处理步骤

(1) 通过 Probe 命令 **display system internal telemetry** 查看采样路径是否有最小采样周期。

例如，以下显示结果中，采样路径 route/ipv4routes 配置的采样周期（Sampling interval，100 毫秒）小于生效的采样周期（Effective sampling interval，5 秒），说明该采样路径存在最小采样周期（5 秒），此时最小采样周期生效。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe] display system internal telemetry
Current-time: 2021-12-25T15:51:45.530
--------------------Subscription s----------------------
Subscription mode: non-gNMI
DSCP value: 0
Source address or interface: Not configured
Telemetry data model:  2-layer
Encoding: JSON
Protocol: GRPC
Sensor group: s
  Sampling interval: 100 milliseconds
  Sampling type         Effective sampling interval   Sensor path
```

```
  Periodic              5 seconds                    route/ipv4routes
Destination group: d
...
[Sysname-probe] quit
```

(2) 确认设备是否处于 CPU 繁忙状态。

通过 **display cpu-usage** 命令查看 CPU 利用率。

```
[Sysname] display cpu-usage
Slot 0 CPU 0 CPU usage:
       70% in last 5 seconds
       62% in last 1 minute
       60% in last 5 minutes
...
```

如果主设备/全局主用主控板的 CPU 利用率超过 60%，将会影响 Telemetry 功能的采样效率，导致设备不能在配置的采样周期内完成数据采样。用户可以选择：

- 等待 CPU 利用率降到 60%以下。
- 减少配置的采样路径数量，以降低 CPU 利用率。

(3) 确认是否订阅了 ifmgr/interfaces、路由类或统计类采样路径。

进入 Telemetry 视图，通过 **display this** 命令查看配置。

```
[Sysname] telemetry
[Sysname-telemetry] display this
#
telemetry
 sensor-group s
  sensor path route/ipv4routes
 destination-group d
  ipv4-address 192.168.79.155 port 50051
 subscription s
  sensor-group s sample-interval 5
  destination-group d
#
```

说明

- 统计类采样路径通常会包含 statistics 节点，例如 ifmgr/statistics。
- 路由类采样路径通常会包含 route 节点，例如 route/ipv4routes。

当存在 ifmgr/interfaces、路由类或统计类采样路径时，在网管侧查看设备上送给采集器的相邻的两个订阅报文之间的时间差是否为命令行配置的采样周期的整数倍。

假设，设备上为采样路径 route/ipv4routes 配置的采样周期为 5 秒，上送给采集器的两个订阅报文之间的时间差为两个 Timestamp（单位为毫秒）字段的差 = (1641482427751 – 1641482417751) / 1000 = 10 秒，是 5 秒的整数倍。

这就说明，该采样路径的采集数据量过大，需要使用多个配置的采样周期才能上送数据。

```
Producer-Name: H3C
...
Sensor-Path: route/ipv4routes
```

```
Json-Data: {"Notification":{"Timestamp":"1641482417751",...

Producer-Name: H3C
...
Sensor-Path: route/ipv4routes
Json-Data: {"Notification":{"Timestamp":"1641482427751",...
```

(4) 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

5. 告警与日志

相关告警

无

相关日志

无