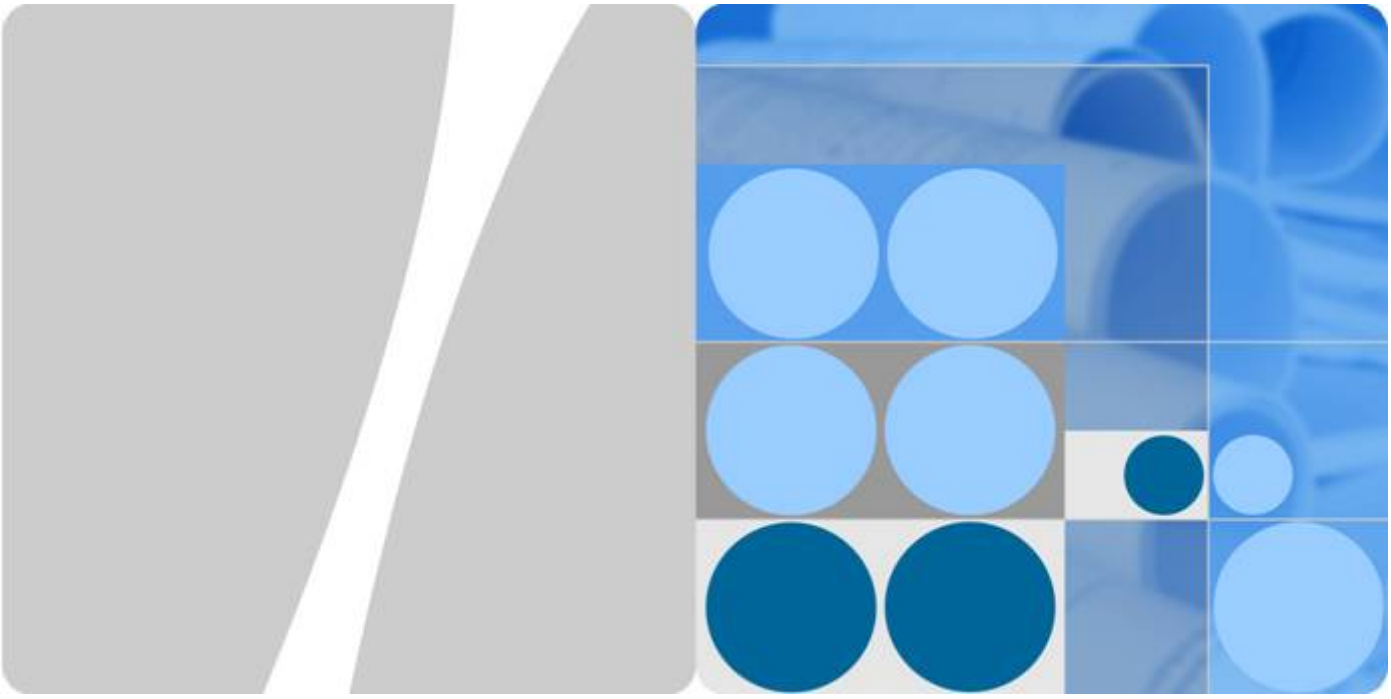


Huawei AR2200-S 系列企业路由器

V200R002C01

故障处理

文档版本　01

发布日期　2012-04-20

华为技术有限公司

版权所有 © 华为技术有限公司 2012。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档针对 AR2200-S 设备的各类业务，从常见原因、故障诊断流程、故障处理步骤、相关告警与日志等方面分析介绍了常见故障现象的定位思路，并给出了典型案例的解决方法。

本文档主要适用于以下工程师：

- 系统维护工程师
- 调测工程师
- 网络监控工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

华为专有和保密信息
版权所有 © 华为技术有限公司

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-04-20)

第一次正式发布。

版权所有 © 华为技术有限公司

目 录

前 言 ii

1 硬件类 1

1.1 SD 卡故障处理 2

1.1.1 SD 卡无法写入的定位思路 2

1.2 单板注册失败故障处理 3

1.2.1 单板注册失败的定位思路 3

2 系统类 6

2.1 CPU 故障处理 7

2.1.1 CPU 占用率高的定位思路 7

2.2 Telnet 故障处理 11

2.2.1 Telnet 登录失败的定位思路 11

2.3 SSH 故障处理 14

2.3.1 通过 SSH 登录 SSH Server 失败的定位思路 14

2.4 镜像故障处理 18

2.4.1 配置端口镜像后监控设备看不到镜像报文的定位思路 18

2.4.2 配置流镜像后监控设备看不到镜像报文的定位思路 21

2.4.3 故障案例 24

2.5 SNMP 故障处理 27

2.5.1 SNMP 无法连接的定位思路 27

2.5.2 网管无法收到主机发送的告警的定位思路 29

2.6 RMON 故障处理 31

2.6.1 网管无法接收 RMON 告警信息的定位思路 31

2.7 NQA 故障处理 34

2.7.1 无法启动 UDP Jitter 测试的定位思路 34

2.7.2 UDP Jitter 测试结果有 drop 记录的定位思路 35

2.7.3 UDP Jitter 测试结果有 busy 记录的定位思路 37

2.7.4 UDP Jitter 测试结果有 timeout 记录的定位思路 38

2.7.5 UDP Jitter 测试结果 failed、no result 或者有丢包的定位思路 40

2.8 NTP 故障诊断思路 42

2.8.1 时钟未同步的定位思路 42

2.9 CWMP 故障处理 43

2.9.1 通过 CWMP 管理设备失败的定位思路 44

版权所有 © 华为技术有限公司

3 物理对接及接口类.....47
3.1 Eth-Trunk 接口故障处理.....48
3.1.1 Eth-Trunk 转发不通的定位思路.....48
3.1.2 故障案例.....52
4 局域网类.....55
4.1 VLAN 故障处理.....56
4.1.1 VLAN 内不能互通的定位思路.....56
4.2 MAC 表故障处理.....60
4.2.1 设备上无法创建正确的 MAC 表项故障处理思路.....60
4.3 MSTP 故障处理.....64
4.3.1 MSTP 拓扑变化导致业务中断的定位思路.....64
4.4 透明网桥故障处理.....70
4.4.1 桥组内二层转发不通的定位思路.....70
4.4.2 集成路由桥接转发不通的定位思路.....72
5 广域网类.....78
5.1 E1/T1 故障处理.....79
5.1.1 E1/T1 接口物理状态正常但数据收发异常的定位思路.....79
5.2 FR 故障处理.....83
5.2.1 FR 链路协议 UP，但无法 ping 通对端的定位思路.....83
5.2.2 故障案例.....88
5.3 MFR 故障处理.....89
5.3.1 MFR 链路协议 UP，但无法 ping 通对端的定位思路.....89
5.3.2 故障案例.....94
5.4 DCC 故障处理.....95
5.4.1 ISDN 拨号不通的定位思路（发起呼叫）.....95
5.4.2 ISDN 拨号不通的定位思路（接受呼叫）.....99
5.5 ISDN 故障处理.....102
5.5.1 ISDN 接口建立链路失败的定位思路.....103
5.6 PPPoE 故障处理.....107
5.6.1 PPPoE 拨号失败定位思路.....107
5.7 PPP 故障处理.....111
5.7.1 PPP 接口协议 Down 的定位思路.....111
5.8 xDSL 故障处理.....117
5.8.1 ADSL 接口在 ATM 模式下报文转发不通的定位思路.....117
5.8.2 G.SHDSL 接口在 ATM 模式下报文转发不通的定位思路.....120
5.9 3G 故障处理.....124
5.9.1 拨号参数配置 OK，3G 呼叫失败的定位思路.....124
6 语音类.....130
6.1 语音故障处理.....131
6.1.1 摘机后无拨号音的定位思路.....131
6.1.2 通话质量低的定位思路.....132

版权所有 © 华为技术有限公司

6.1.3 呼叫失败的定位思路.....134
6.1.4 SIP 接口故障的定位思路.....137
7 IP 转发及路由类.....140
7.1 Ping 故障处理.....141
7.1.1 Ping 不通问题的定位思路.....141
7.1.2 故障案例.....148
7.2 DHCP 故障处理.....150
7.2.1 客户端无法获取 IP 地址的定位思路（AR2200-S 作为 DHCP Server）.....150
7.2.2 客户端无法获取 IP 地址的定位思路（AR2200-S 作为 DHCP Relay）.....153
7.3 RIP 故障处理.....157
7.3.1 RIP 没有学到部分或全部路由的定位思路.....157
7.3.2 设备没有发送部分或全部 RIP 路由的定位思路.....160
7.4 OSPF 故障处理.....163
7.4.1 OSPF 邻居 Down 的定位思路.....163
7.4.2 OSPF 邻居无法达到 FULL 状态的定位思路.....167
7.4.3 故障案例.....171
8 组播类.....177
8.1 三层组播故障处理.....178
8.1.1 组播业务不通的定位思路.....178
8.1.2 PIM 邻居 Down 的定位思路.....181
8.1.3 PIM-SM 网络中 RPT 无法正常转发数据的定位思路.....183
8.1.4 PIM-SM 网络中 SPT 无法正常转发数据的定位思路.....188
8.1.5 MSDP 对等体无法正确建立（S,G）表项的定位思路.....192
8.1.6 组播设备无法正常建立 IGMP 表项的定位思路.....196
9 QoS 类.....201
9.1 流策略故障处理.....202
9.1.1 流策略不生效的定位思路.....202
9.2 优先级映射故障处理.....205
9.2.1 报文未进入正确队列的定位思路.....205
9.2.2 优先级映射结果不正确的定位思路.....208
9.2.3 故障处理案例.....211
9.3 流量监管故障处理.....215
9.3.1 基于类的流量监管不生效.....215
9.3.2 基于接口的流量监管限速不准确的定位思路.....215
9.3.3 故障处理案例.....219
9.4 流量整形故障处理.....220
9.4.1 基于队列的流量整形结果不正确的定位思路.....220
9.4.2 故障处理案例.....223
9.5 拥塞避免故障处理.....225
9.5.1 拥塞避免不生效的定位思路.....225
9.6 拥塞管理故障处理.....228

版权所有 © 华为技术有限公司

9.6.1 拥塞管理无效的定位思路.....228
9.6.2 故障处理案例.....231
10 安全类.....234
10.1 AAA 故障处理.....235
10.1.1 RADIUS 用户认证失败的定位思路.....235
10.1.2 HWTACACS 用户认证失败的定位思路.....239
10.1.3 故障案例.....244
10.2 ARP 安全故障处理.....250
10.2.1 合法用户的 ARP 表项被修改的定位思路.....250
10.2.2 网关地址被仿冒的定位思路.....252
10.2.3 ARP 报文攻击导致用户流量中断的定位思路.....255
10.2.4 IP 扫描攻击的定位思路.....257
10.2.5 ARP 学习失败的定位思路.....259
10.3 NAC 故障处理.....261
10.3.1 802.1x 认证失败的定位思路.....261
10.3.2 MAC 认证失败的定位思路.....265
10.3.3 MAC 旁路认证失败的定位思路.....268
10.3.4 Web 认证失败的定位思路.....269
10.4 DHCP Snooping 故障处理.....272
10.4.1 DHCP Snooping 导致用户无法上线的定位思路.....272
10.5 防火墙故障处理.....274
10.5.1 用户通过流量监测工具发现网络中存在大量的 SYN 报文.....274
10.6 ACL 故障处理.....276
10.6.1 ACL 不起作用引起包过滤防火墙失效的定位思路.....276
10.7 NAT 故障处理.....278
10.7.1 NAT Outbound 故障现象：内网用户无法访问公网.....278
10.7.2 NAT Server 故障现象：外网主机无法访问内网服务器.....280
10.7.3 两次 NAT 故障现象：内网重叠主机无法访问外网服务器.....283
10.8 PKI 故障处理.....287
10.8.1 获取 CA 证书失败的定位思路.....287
10.8.2 申请本地证书失败的定位思路.....289
10.8.3 CRL 获取失败的定位思路.....291
11 可靠性类.....294
11.1 接口备份故障处理.....295
11.1.1 接口备份失效的定位思路.....295
11.1.2 故障案例.....298
11.2 BFD 故障处理.....299
11.2.1 BFD 会话无法 Up 的定位思路.....300
11.2.2 BFD 会话检测 Down 影响接口转发的定位思路.....303
11.2.3 修改 BFD 会话检测参数不生效的定位思路.....305
11.2.4 动态 BFD 会话没有创建成功的定位思路.....307

版权所有 © 华为技术有限公司

11.3 VRRP 故障处理.....309
11.3.1 故障案例.....309
12 VPN 类.....313
12.1 GRE 故障处理.....314
12.1.1 无法 Ping 通对端 Tunnel 接口 IP 地址的定位思路.....314
12.1.2 故障案例.....317
12.2 IPSec 故障处理.....320
12.2.1 采用 Manual 方式无法建立安全联盟的定位思路.....320
12.2.2 采用 IKE 方式无法建立安全联盟的定位思路.....324
12.2.3 采用安全策略模板配置 IPSec 失败的定位思路.....330
12.2.4 IPSec 的 NAT 穿越的定位思路.....337
12.2.5 GRE over IPSec 的定位思路.....343
12.2.6 采用 IPSec 虚拟隧道方式无法建立安全联盟的定位思路.....350
12.2.7 故障处理案例.....354
12.3 SSL VPN 故障处理.....356
12.3.1 用户无法登陆 SSL VPN 网关设备的定位思路.....356
12.4 DSVPN 故障处理.....359
12.4.1 Spoke 向 Hub 注册失败的定位思路.....360
12.4.2 分支间进行路由学习场景下 Spoke 与 Spoke 之间无法通信的定位思路.....363
12.4.3 分支只有到总部的汇聚路由场景下 Spoke 与 Spoke 之间无法通信的定位思路.....367

版权所有 © 华为技术有限公司

1 硬件类

关于本章

1.1 SD 卡故障处理

1.2 单板注册失败故障处理

版权所有 © 华为技术有限公司

1.1 SD 卡故障处理

1.1.1 SD 卡无法写入的定位思路

常见原因

本类故障的常见原因主要包括：

- SD 卡从卡槽内弹出
- SD 卡存储空间已满
- SD 卡损坏

故障诊断流程

无

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 SD 卡是否被弹出

请检查主控面板上 SD 卡指示灯是否常亮或者闪烁。如果指示灯常灭，说明 SD 卡被弹出。如果在用户视图下执行 **dir** 命令，显示信息中无“sd0：”，也能说明 SD 卡被弹出。

- 如果 SD 卡被弹出，请将 SD 卡压回卡槽内。
- 如果 SD 卡在位，请执行步骤 2。

步骤 2 检查 SD 卡是否有足够的空闲空间

在用户视图下执行 **dir sd0:**命令，检查 SD 卡上是否还有足够的空闲空间(free)。

- 如果已经没有足够的剩余空间，则需要删除部分 SD 上的文件以释放空间，可以将 SD 卡上的文件下载到本地存储设备后，删除 SD 卡上的文件。
- 如果执行 dir sd0:命令无法显示出当前 SD 卡的剩余空间，或者剩余空间足够写入的文件大小，但文件仍然无法写入。说明 SD 卡可能已经损坏，请按照以下步骤更换 SD 卡。

1. 按压 SD 卡，使其从卡槽内弹出。取出损坏的 SD 卡设备放入防静电袋中。
2. 插入新的 SD 卡。将 SD 卡按入卡槽，使其被卡紧不能被拔出且 SD 卡在位指示灯点亮。
3. 检查 SD 卡的运行状态，观察日志信息。当 SD 卡插入时，设备会产生日志信息。此时使用 **dir** 命令，能够显示 SD 卡设备，则表示新 SD 卡正常安装。

版权所有 © 华为技术有限公司

- 如果更换 SD 卡后，SD 卡仍然无法写入，请执行步骤 3。

步骤 3 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

DEV/4/MEMORYCARDEVENT： Register the device sd0: successfully

DEV/4/MEMORYCARDEVENT: Device sd0: unregister successfully

相关日志

无

1.2 单板注册失败故障处理

1.2.1 单板注册失败的定位思路

常见原因

本类故障的常见原因主要包括：

- 单板尚未完成启动，即正在启动中
- 单板发生复位

故障诊断流程

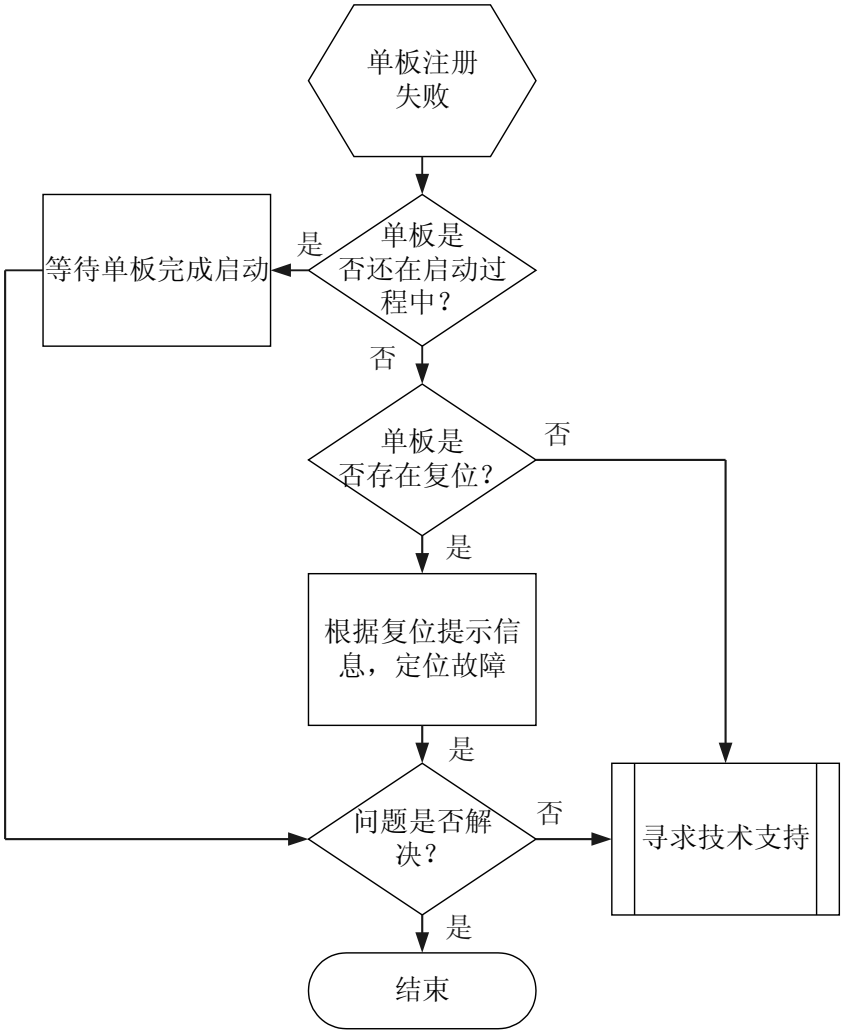
单板无法注册的定位思路如下：

- 检查单板是否在启动过程中。
- 启动完成后，检查单板是否为注册失败。
- 检查单板是否发生复位，根据复位原因定位故障。

详细处理流程如图 1-1 所示。

版权所有 © 华为技术有限公司

图 1-1 单板注册故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查单板是否仍然在启动过程中

单板从上电到完成注册需要一段时间，叫做启动时间。各种单板的启动时间如下：

- 主控板启动时间在 3 分钟内，如果是升级系统软件后重新启动设备，启动时间不超过 5 分钟。
- 接口板启动时间在 5 分钟之内，如果需要更新系统软件，启动时间不超过 10 分钟。
- 如果未超出单板的启动时间，请等待。

版权所有 © 华为技术有限公司

- 如果已经超出启动时间，执行 **display device** 检查单板状态。如果显示信息中“Register”的信息为“Unregistered”即单板未注册上请执行步骤 2。

步骤 2 检查单板是否存在复位现象。

- 如果执行 **display reset-reason** [**slot** *slot-id*]命令，无单板的复位信息，说明单板一次也没有注册过，这时通常需要通过串口线检查单板加载是否正确，详细的故障处理步骤请参考“单板加载故障处理”。
- 如果执行 **display reset-reason** [**slot** *slot-id*]命令，有单板复位原因的显示信息，请根据实际显示的复位原因，解决单板复位故障。

  如果单板复位的故障排除后，单板仍然无法注册，请执行步骤 3。

步骤 3 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

2 系统类

关于本章

2.1 CPU 故障处理

2.2 Telnet 故障处理

2.3 SSH 故障处理

2.4 镜像故障处理
介绍了端口镜像和流镜像组网中常见故障的定位思路和案例。

2.5 SNMP 故障处理

2.6 RMON 故障处理

2.7 NQA 故障处理

2.8 NTP 故障诊断思路

2.9 CWMP 故障处理

版权所有 © 华为技术有限公司

2.1 CPU 故障处理

2.1.1 CPU 占用率高的定位思路

常见原因

CPU 占用率，就是一个时间段内，CPU 执行代码的时间与时间段总长度的比率。CPU 占用率常常是衡量设备性能的重要指标之一。

CPU 占用率高，是设备本身的一种现象，直观表现为 **display cpu-usage** 命令查询结果中整机 CPU 占用率“CPU usage”偏高，如超过 70%。在网络运行中 CPU 高常常会导致其他业务异常，如 BGP 震荡、VRRP 频繁切换、甚至设备无法登录。以下讨论的原因及步骤基于 CPU 占用率高这个现象。

通常，整机 CPU 占用率过高，是由于某些任务的 CPU 占用率居高不下导致的。具体导致某任务 CPU 占用率高的可能原因：

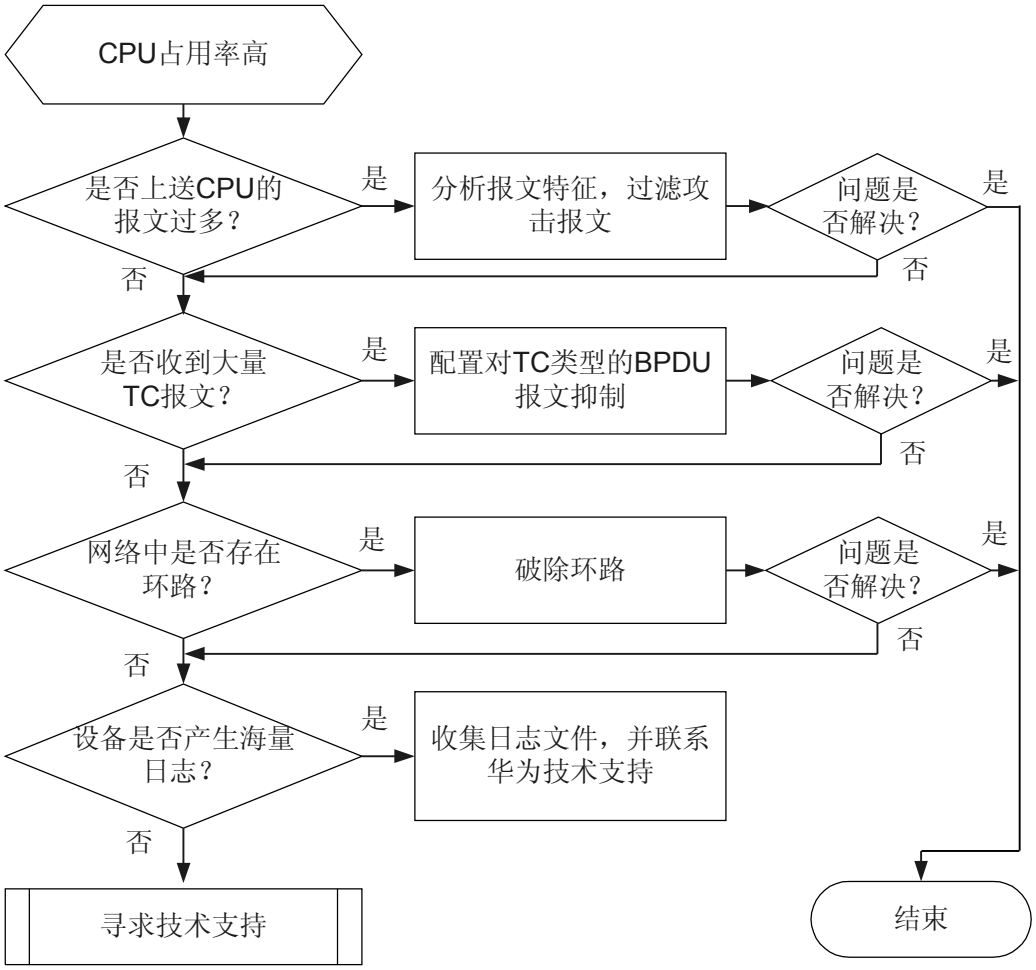
- 上送 CPU 报文过多，如环路或 DoS 报文攻击
- STP 网络频繁震荡，收到大量 TC 报文，造成设备频繁删除 MAC 表和 ARP 表项
- 设备产生海量日志，占用大量 CPU 资源

故障诊断流程

详细处理流程如图 2-1 所示。

版权所有 © 华为技术有限公司

图 2-1 CPU 占用率高故障诊断流程图



故障处理步骤

说明

请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。

以下的步骤之间并没有严格的顺序关系，实际操作中并不一定要遵守文中所给的顺序。

设备型号不同，以下步骤中命令的显示信息也会有差异，请以设备实际显示信息为准。文中示例旨在告诉读者如何查看相关信息。

操作步骤

步骤 1 检查占用 CPU 高的任务名称

执行命令 **display cpu-usage**，查看各任务的 CPU 占用率。

记录 CPU 占用率超过 70%的任务名称。

说明

这个取值并非绝对数值，有可能某些任务执行时就需要占用 70%的 CPU 而对业务不会造成影响，也有可能某些任务占用 CPU 30%时就会对业务造成影响。应该根据实际情况判断。

版权所有 © 华为技术有限公司

步骤 2 检查是否上送 CPU 的报文太多

执行命令 **display cpu-defend statistics**，查看上送 CPU 报文的统计信息，关注丢弃计数。

```
<Huawei> display cpu-defend statistics all
-------------------------------------------------------------------
Packet Type                Pass Packets         Drop Packets
-------------------------------------------------------------------
8021X                                 0                    0
arp-miss                              1                    0
arp-reply                             5                    0
arp-request                     1450113                25597
bfd                                   0                    0
bgp                                   0                    0
dhcp-client                      114693                136586
dhcp-server                           0                    0
dns                                   0                    0
fib-hit                               0                    0
ftp                                 717                    0
fw-dns                                0                    0
fw-ftp                                0                    0
fw-http                               0                    0
fw-rtsp                               0                    0
fw-sip                                0                    0
gvrp                                  0                    0
http                                798                    0
hw-tacacs                             0                    0
icmp                                 10                    0
igmp                                  0                    0
ipsec                                 0                    0
isis                                  0                    0
lacp                                  0                    0
lldp                              33959                    0
ntp                                   0                    0
ospf                                1569                    0
pim                                   0                    0
pppoe                                 0                    0
radius                                0                    0
rip                                   0                    0
snmp                                  0                    0
ssh                                   0                    0
stp                                   0                    0
tcp                                7671                    0
telnet                            71149                    0
ttl-expired                         656                    0
udp-helper                            0                    0
unknown-multicast                     6                    0
unknown-packet                    94189                    0
vrrp                                  0                    0
-------------------------------------------------------------------
```

- 如果某种类型报文“Drop”计数较大，且对应上一步中占用的 CPU 使用率较高，可以判断为发生了报文攻击。请执行步骤 6。
- 如果没有发现有流量过大的报文，请执行步骤 3。

步骤 3 检查是否 TC 报文过多

支持 STP 的设备上，STP 使能情况下，设备在接收到 TC-BPDU 报文时，会删除 MAC 地址表项和 ARP 表项。如果有人伪造 TC-BPDU 报文恶意攻击，设备短时间内会收到很多 TC-BPDU 报文，频繁的删除操作会导致 CPU 占用率比较高。

执行命令 **display stp**，查看接口下收到的 TC 报文和 TCN 报文计数。

```
<Huawei> display stp interface Eth2/0/1
----[CIST][Port2(Ethernet2/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=199999
```


版权所有 © 华为技术有限公司

```
Designated Bridge/Port   :4096.00e0-fc01-0005 / 128.2
Port Edged               :Config=default / Active=disabled
Point-to-point           :Config=auto / Active=true
Transit Limit            :147 packets/hello-time
Protection Type          :None
Port STP Mode            :MSTP
Port Protocol Type       :Config=auto / Active=dot1s
PortTimes                :Hello 2s MaxAge 20s FwDly 15s RemHop 20
TC or TCN send           :1
TC or TCN received       :0
BPDU Sent                :124008
         TCN: 0, Config: 0, RST: 0, MST: 124008
BPDU Received            :0
         TCN: 0, Config: 0, RST: 0, MST: 0
```

- 如果该值很大，系统视图下执行命令 **stp tc-protection** 配置对 TC 类型 BPDU 报文的抑制。配置此命令后，默认每个 Hello 周期处理 3 个 TC 报文。可以根据实际情况通过 **stp tc-protection threshold** 命令指定处理的报文数量门限值，可以通过 **stp timer hello** 命令修改 Hello 周期的时长。

  ```
  [Huawei] stp tc-protection
  [Huawei] stp tc-protection threshold 5
  [Huawei] stp timer hello 200
  ```

- 如果 TC 报文数量不多，请执行步骤 4。

步骤 4 检查网络是否有环路

当设备的某个 VLAN 中包含较多接口时，如果有两个接口形成环路，则报文会在多个接口之间一直转发，会导致 CPU 占用率上升。

执行命令 **display current-configuration**，查看是否使能了 MAC 地址漂移告警功能。

```
#
 loop-detect eth-loop alarm-only
#
```

- 如果没有，执行命令 **loop-detect eth-loop alarm-only** 配置当发生 MAC 地址漂移时产生告警。此时如果网络中有环路，当设备两个接口学习到同一个 MAC 表项时，会产生告警。如：

  ```
  Feb 22 2011 18:42:50 Huawei L2IFPPI/4/MAC_FLAPPING_ALARM:OID
  1.3.6.1.4.1.2011.5.25.42.2.1.7.12The mac-address has flap value .
  (L2IfPort=0,entPhysicalIndex=0,  BaseTrapSeverity=4, BaseTrapProbableCause=549,
  BaseTrapEventType=1,  MacAdd=0000-c0a8-0101,vlanid=100,
  FormerIfDescName=Ethernet1/0/0,CurrentIfDescName=Ethernet1/0/1,DeviceName=HUAWEI)
  ```

  根据告警提示信息，查看相应的接口连接以及组网需求。

  - 如果不需要环网，根据组网图，将其中一个端口 shutdown 处理。
  - 如果确实需要环网，关闭 Loop Detection 功能，并启动 STP 等破环协议。

- 如果设备已经配置了 **loop-detect eth-loop alarm-only**，但是没有看到告警，请执行步骤 5。

步骤 5 检查设备是否产生海量日志

某些异常情况下如受到攻击、运行中发生了错误、端口频繁 Up/Down 等，设备会不停打印诊断信息或日志信息。此时对存储器要进行频繁的读写操作，会造成 CPU 占用率升高。

执行命令 **display logbuffer**，查看是否有大量的异常日志。如某一条信息不断地大量重复出现。执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

版权所有 © 华为技术有限公司

- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.2 Telnet 故障处理

2.2.1 Telnet 登录失败的定位思路

常见原因

本类故障的常见原因主要包括：

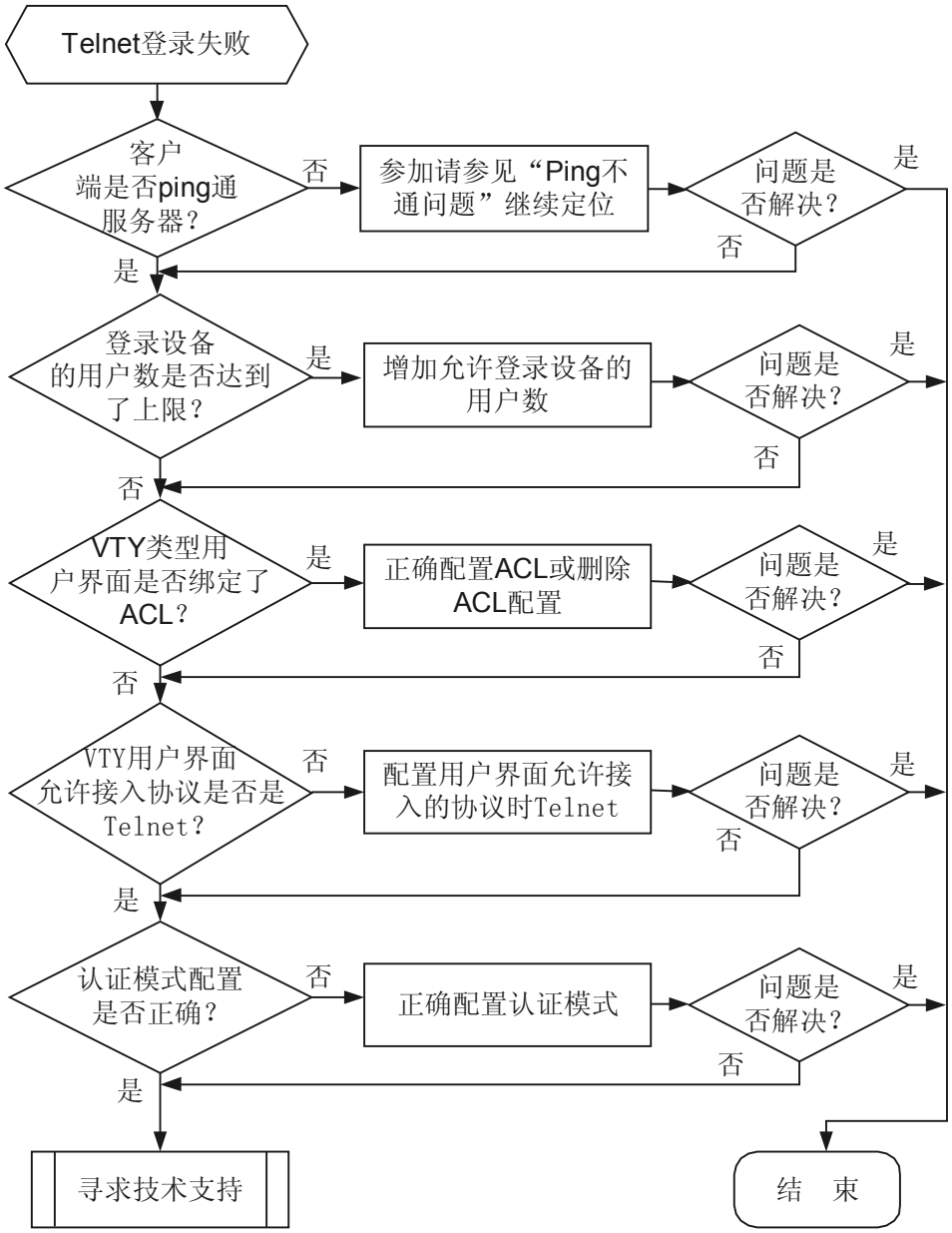
- 路由不可达，客户端和服务器无法建立 TCP 连接。
- 登录设备的用户数到达了上限。
- VTY 用户界面下绑定了 ACL。
- VTY 用户界面下允许接入的协议不正确，如配置为 **protocol inbound ssh** 时，使用 Telnet 将无法登录。

故障诊断流程

故障诊断流程如图 2-2 所示。

版权所有 © 华为技术有限公司

图 2-2 Telnet 故障流程诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查客户端能否 Ping 通服务器。

在客户端使用 **ping** 命令查看网络连接情况。如果不能 Ping 通，则 Telnet 连接也将失败。

如果 Ping 不通，请参见 **Ping 不通问题**继续定位，使 Telnet 客户端能 Ping 通服务器端。

版权所有 © 华为技术有限公司

步骤 2 检查登录设备的用户数是否到达了上限。

从 Console 口登录到设备，执行命令 **display users**，查看当前的 VTY 通道是否全部被占用。缺省情况下，VTY 通道允许的最大用户数是 5 个，可以先执行命令 **display user-interface maximum-vty**，查看当前 VTY 通道允许的最大用户数。

```
<Huawei> display user-interface maximum-vty
 Maximum of VTY user:5
<Huawei> display users
  User-Intf    Delay    Type   Network Address     AuthenStatus    AuthorcmdFlag
+ 0   CON 0   00:00:00                                              no
  Username : Unspecified

  34  VTY 0   00:13:39  TEL    10.138.78.107                         no
  Username : Unspecified
```

如果当前的用户数已经达到上限，可以执行命令 **user-interface maximum-vty** *vty-number*，将 VTY 通道允许的最大用户数扩展到 15 个。

```
<Huawei> system-view
[Huawei] user-interface maximum-vty 15
```

步骤 3 查看设备上 user-interface vty 下是否绑定了 ACL。

```
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] display this
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode aaa
 user privilege level 3
 idle-timeout 0 0
```

如果绑定了 ACL，但 ACL 规则中未指定 **permit** 客户端的 IP 地址，则使用 Telnet 登录设备时将失败。即，如果需要使用某 IP 地址通过 Telnet 登录到设备，必须在 **user-interface vty** 下绑定的 ACL 规则中配置允许该 IP 地址。

步骤 4 查看 user-interface vty 下允许接入的协议配置是否正确。

```
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] display this
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 idle-timeout 0 0
 protocol inbound ssh
```

命令 **protocol inbound** { **all** | **ssh** | **telnet** }用来配置允许登录接入用户类型的协议。**protocol inbound telnet** 为缺省配置。

- 如果配置为 **protocol inbound ssh**，使用 Telnet 将无法登录。
- 如果配置为 **protocol inbound all**，则使用 Telnet 或 SSH 都可以登录。

步骤 5 检查用户界面视图下是否设置登录认证。

- 如果使用命令 **authentication-mode password** 配置了 VTY 通道下的登录认证方式为 **password**，则必须使用命令 **set authentication password** 设置认证密码。
- 如果使用命令 **authentication-mode aaa** 设置认证方式为 **aaa**，则必须使用命令 **local-user** 创建 AAA 本地用户。

步骤 6 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警与日志

相关告警

无

相关日志

无

2.3 SSH 故障处理

2.3.1 通过 SSH 登录 SSH Server 失败的定位思路

常见原因

本类故障的常见原因主要包括：

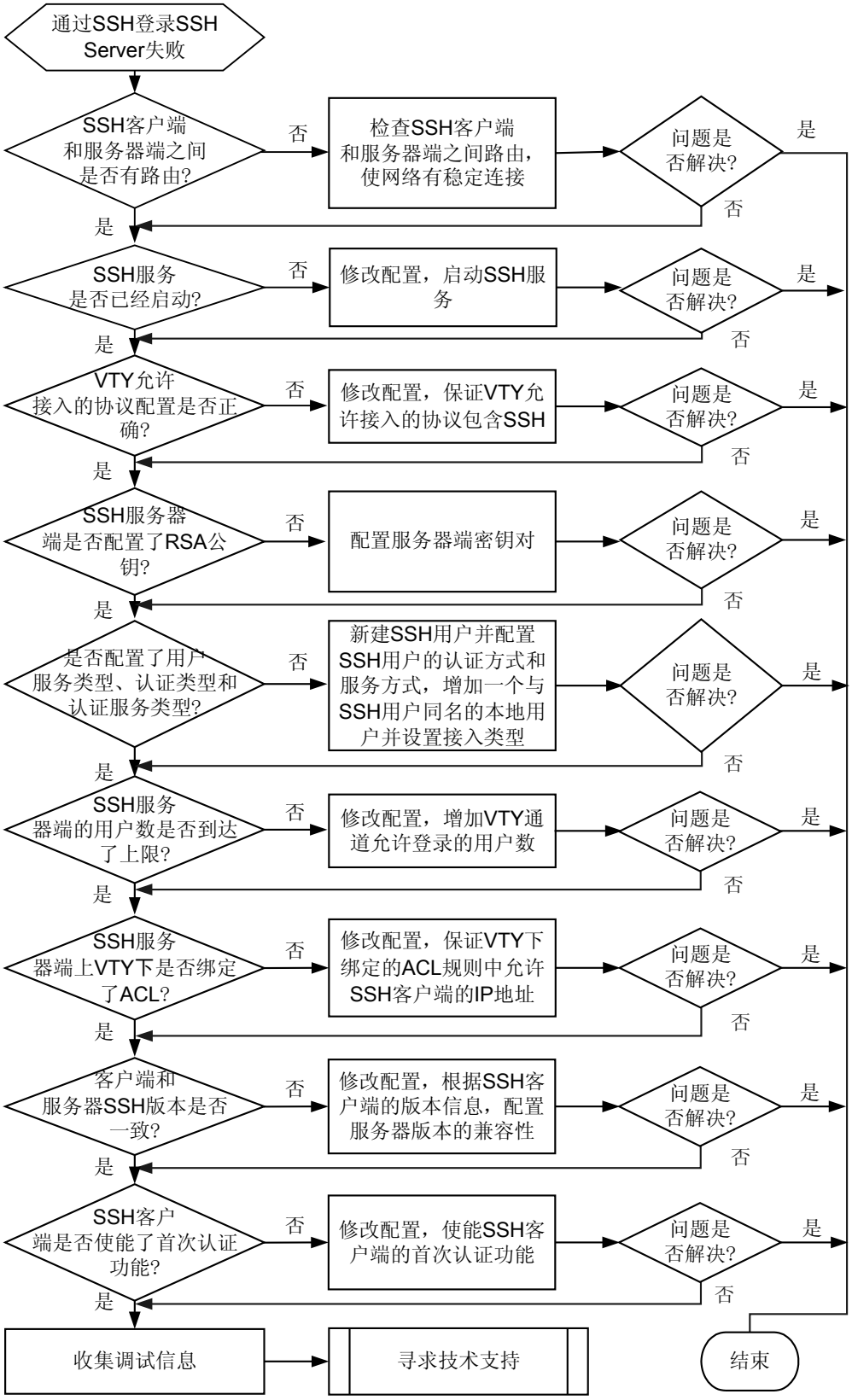
- SSH Client 与 SSH Server 之间没有可达路由，无法建立 TCP 连接。
- SSH 服务未启动。
- 用户界面 VTY 接口下未绑定 SSH 协议。
- 没有配置 SSH 服务器和客户端的 RSA 公钥。
- 没有配置用户服务类型、认证类型、用户认证服务类型。
- 设备上登录用户数达到允许用户数的上限。
- **user-interface vty** 下绑定了 ACL 规则。
- 服务器端与客户端 SSH 版本不一致。
- 客户端未使能 SSH 客户端首次认证功能。

故障诊断流程

可按照图 2-3 排除此类故障。

版权所有 © 华为技术有限公司

图 2-3 通过 SSH 登录 SSH Server 失败故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 SSH 客户端和服务器之间网络是否畅通。

分别在 SSH 客户端和服务器上使用 **ping** 命令查看网络连接情况。如果不能 ping 通，则 SSH 连接也将失败。

检查网络中是否有不稳定连接，如报文丢失、登录时断时好的情况。请参见 **Ping 不通问题**继续定位，使 SSH 客户端和服务器端之间的网络有稳定连接。

步骤 2 查看 SSH 服务器端的 SSH 服务是否启动。

通过 Telnet 方式登录 SSH 服务器端，执行命令 **display ssh server status**，查看 SSH 服务器端配置信息。这里以 SFTP 服务为例。

```
<Huawei> display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH Authentication retries           :3 times
 SFTP server                          :Disable
```

可以看到，SFTP 没有使能。只有当系统启动了 SSH 服务，用户才能登录。执行如下命令，使能 SSH 服务器。

```
<Huawei> system-view
[Huawei] sftp server enable
```

步骤 3 在 SSH 服务器端上查看 user-interface vty 下允许接入的协议配置是否正确。

```
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] display this
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 idle-timeout 0 0
 protocol inbound ssh
```

命令 **protocol inbound** { **all** | **ssh** | **telnet** }用来配置允许登录接入用户类型的协议。**protocol inbound telnet** 为缺省配置。如果配置为 **protocol inbound telnet**，使用 SSH 将无法登录；如果配置为 **protocol inbound ssh** 或 **protocol inbound all**，则使用 SSH 都可以登录。

步骤 4 检查在 SSH 服务器端是否配置了 RSA 公钥。

设备作为 SSH 服务器时，必须配置本地密钥对。

在 SSH 服务器端上执行命令 **display rsa local-key-pair public** 查看当前服务器端密钥对信息。如果显示信息为空，则表明没有配置服务器端密钥对，执行命令 **rsa local-key-pair create** 创建。

```
[Huawei] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]: 768
Generating keys...
.........................++++++++
.++++++++
```


版权所有 © 华为技术有限公司

```
..............+++++++++
......+++++++++
```

步骤 5 （可选）检查 SSH 服务器端上是否配置了 SSH 用户。

SSH 服务器端上应该正确配置了 SSH 用户。执行命令 **display ssh user-information**，查看 SSH 用户的配置信息。如果不存在配置信息，请在 AAA 视图下分别执行命令 **local-user** *user-name* **password** *password* 和 **local-user service-type ssh**，新建 SSH 用户。

说明

对于 SFTP 服务，还需在 AAA 视图下执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置 SSH 用户的 SFTP 服务授权目录。

- 创建 SSH 用户。

```
[Huawei] aaa
[Huawei] local-user abc password  abc-pass
[Huawei] local-user abc service-type ssh
[Huawei] local-user abc ftp-directory  cfcard:/ssh
```

- SSH 用户的认证方式缺省为 password 认证，可以执行 **ssh user authentication-type** 命令修改 SSH 用户的认证方式。

步骤 6 检查登录 SSH 服务器端的用户数是否到达了上限。

对于 STelnet 与 Telnet 服务，STelnet 用户与 Telnet 用户使用的均是 VTY 通道，VTY 通道是有限资源，最大可配置范围为 5 ～ 15 个。当登录用户数超过 15 个时，设备不再接受新的用户连接。

从 Console 口登录到 SSH 服务器端，执行命令 **display users**，查看当前的 VTY 通道是否全部被占用。缺省情况下，VTY 通道允许的最大用户数是 5 个。

```
<Huawei> display user-interface maximum-vty
 Maximum of VTY user:5
<Huawei> display users
User-Intf    Delay    Type   Network Address     AuthenStatus    AuthorcmdFlag
  34  VTY 0   03:31:35  TEL    10.1.1.1                 pass           no
Username : Unspecified
  35  VTY 1   03:51:58  TEL    10.1.1.2                 pass           no
Username : Unspecified
  36  VTY 2   00:10:14  TEL    10.1.1.3                 pass           no
Username : Unspecified
  37  VTY 3   02:31:58  TEL    10.1.1.4                 pass           no
Username : Unspecified
+ 39  VTY 5   00:00:00  TEL    10.1.1.5                 pass           no
Username : Unspecified
```

如果当前的用户数已经达到上限，可以执行命令 **user-interface maximum-vty** *vty-number*，将 VTY 通道允许的最大用户数扩展到 15 个。

```
<Huawei> system-view
[Huawei] user-interface maximum-vty 15
```

步骤 7 查看 SSH 服务器端上 user-interface vty 下是否绑定了 ACL。

在 SSH 服务器端上执行命令 **user-interface** 进入 SSH 用户会使用的界面视图，执行命令 **display this**，查看 VTY 用户界面是否配置了 ACL 限制，如果配置了 ACL 限制，请记录该 ACL 编号。

在 SSH 服务器端上执行命令 **display acl**，查看该访问控制列表中是否 **deny** 了 SSH Client 的地址。如果 VTY 下绑定了 ACL，但 ACL 规则中未指定 deny 客户端的 IP 地址，则使用 STelnet 或 SFTP 登录设备时将被默认拒绝而导致失败。即，如果需要使用某 IP 地址通过 STelnet 或 SFTP 登录到设备，必须在 user-interface vty 下绑定的 ACL 规则中配置允许该 IP 地址。

版权所有 © 华为技术有限公司

步骤 8 查看 SSH 客户端和服务器上 SSH 版本信息。

在 SSH 服务器上执行命令 **display ssh server status**，查看 SSH 版本信息。

```
<Huawei> display ssh server status
 SSH version                         :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval     :0 hours
 SSH Authentication retries           :3 times
 SFTP server                         :Disable
```

如果使用 SSHv1 版本的客户端登录服务器，则服务器端版本兼容配置需要设置为使能。

```
<Huawei> system-view
[Huawei] ssh server compatible-ssh1x enable
```

步骤 9 查看 SSH 客户端是否使能了首次认证功能。

在 SSH 客户端的系统视图下执行命令 **display this**，查看 SSH 客户端是否配置了命令 **ssh client first-time enable**。

使能 SSH 客户端首次认证功能的目的，是为了当 SFTP 客户端第一次登录 SSH 服务器时，不对 SSH 服务器的 RSA 公钥进行有效性检查，因为此时 SFTP 客户端还没有保存 SSH 服务器的 RSA 公钥。

如果没有使能 SSH 客户端首次认证功能，则 SFTP 客户端第一次登录 SSH 服务器时，由于对 SSH 服务器的 RSA 公钥有效性检查失败，而导致登录服务器失败。

```
<Huawei> system-view
[Huawei] ssh client first-time enable
```

步骤 10 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.4 镜像故障处理

介绍了端口镜像和流镜像组网中常见故障的定位思路和案例。

2.4.1 配置端口镜像后监控设备看不到镜像报文的定位思路

介绍在配置了端口镜像的网络中监控设备看不到镜像报文的故障处理流程和详细的故障处理步骤。

版权所有 © 华为技术有限公司

常见原因

本类故障的常见原因主要包括：

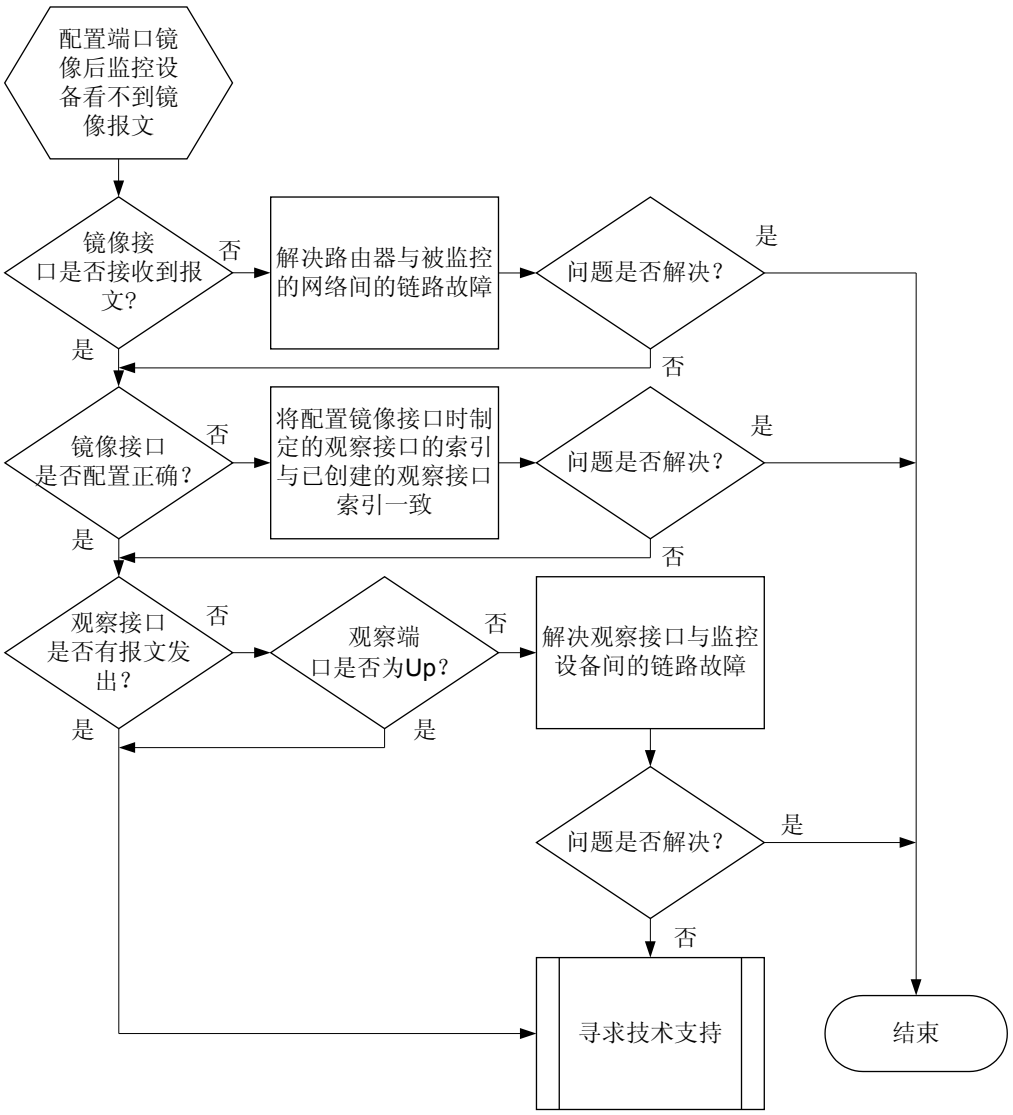
- 镜像端口未收到报文
- 镜像接口或观察接口配置错误，如索引不匹配

故障诊断流程

在配置端口镜像后发现监控设备看不到镜像报文。

详细处理流程如图 2-4 所示。

图 2-4 监控设备看不到镜像报文的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查镜像端口是否接收或者发送报文

执行 **display interface** 命令查看镜像接口的信息，“Input”为镜像接口收到的报文信息，“Output”为镜像接口发送的报文信息。

- 如果镜像接口接收和发送的报文的统计信息均为 0 或者不变化，检查镜像接口的状态。
  - 如果接口状态为 Down，请解决端口故障。
  - 如果接口状态为 Up，镜像接口仍未接收或者发送报文，说明路由器和被监控网络间无流量，不是故障现象。
- 如果镜像接口接收到的报文的统计信息不为 0 且不断变化，请执行步骤 2。

步骤 2 检查镜像端口是否配置正确

配置镜像接口时，指定的观察接口的索引必须与已配置的观察接口的索引一致，可以通过执行命令 **display mirror-port** 命令检查观察接口与镜像接口的对应关系及镜像应用的方向。

- 如果镜像接口配置错误，请在镜像接口的接口视图下执行命令 **mirror（接口视图）** 正确配置镜像接口与观察接口的匹配关系及镜像应用的方向。
- 如果镜像接口配置正确，请执行步骤 3。

步骤 3 检查观察接口是否有发送报文

如果设备上的观察接口没有发出报文，监控设备将无法看到镜像报文。在设备上执行 **display interface** 命令查看观察接口的信息，“Output”为观察接口发出的报文信息。

- 如果观察接口发出的报文的统计信息为 0 或者不变化，说明观察接口没有发出报文，检查观察接口的状态。
  - 如果观察接口的状态为 Down，请解决端口故障。
  - 如果观察接口的状态为 Up，请执行步骤 4。
- 如果观察接口接发出的报文的统计信息不为 0 且不断变化，说明观察接口发出了报文。请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

版权所有 © 华为技术有限公司

相关日志

无

2.4.2 配置流镜像后监控设备看不到镜像报文的定位思路

介绍在配置了流镜像的网络中监控设备看不到镜像报文的故障处理流程和详细的故障处理步骤。

常见原因

本类故障的常见原因主要包括：

- 镜像接口与被监控网络间链路存在故障
- 流策略未被应用或者报文未匹配流策略
- 配置流行为时指定的观察接口索引与已经创建的观察接口索引不一致

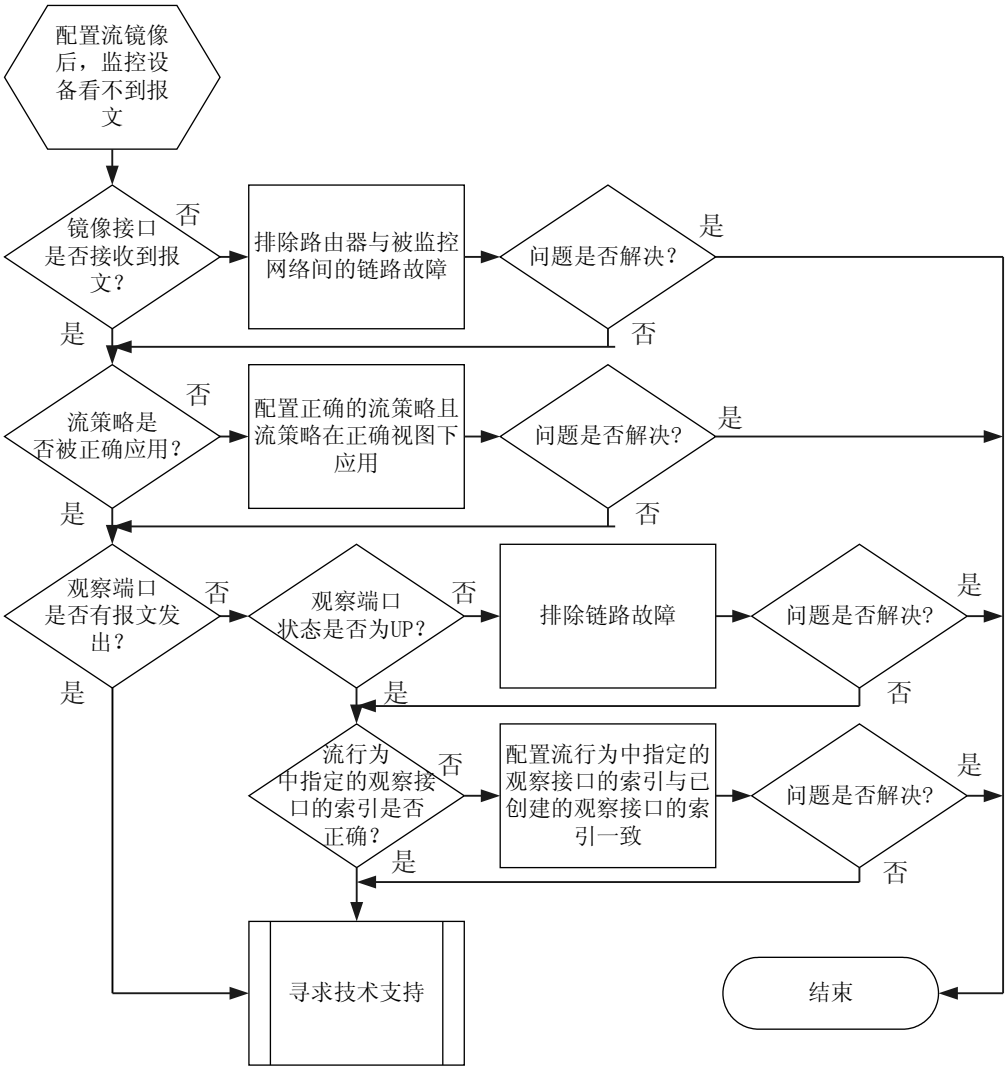
故障诊断流程

在配置流镜像后发现监控设备看不到镜像报文。

详细处理流程如图 2-5 所示。

版权所有 © 华为技术有限公司

图 2-5 流镜像组网中监控设备看不到镜像报文故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查镜像端口是否接收到报文

执行 **display interface** 命令查看镜像接口的信息，“Input”为镜像接口收到的报文信息。

- 如果镜像接口接收到的报文的统计信息为 0 或者不变化，此时路由器与被监控的网络之间可能存在链路故障，如端口 Down 等。
- 如果镜像接口接收到的报文的统计信息不为 0 且不断不变化，请执行步骤 2。

步骤 2 检查流策略是否被正确应用。

版权所有 © 华为技术有限公司

流策略是否被正确应用包含流策略是否被应用及流策略是否正确两个方面，请一次检查配置的正确性。

1. 检查流策略是否被应用

   路由器支持在接口视图或者子接口视图下应用流策略。执行命令 **display traffic-policy** *policy-name* **applied-record** 查看流策略的应用记录。

   - 如果流策略没有在任何视图下被应用，请根据实际组网需要，选择在接口视图或者子接口视图下应用流策略。
   - 如果流策略已经被应用，请检查流策略是否配置正确。

2. 检查流策略配置是否正确。可以通过流策略流量统计的方法检查流策略是否配置正确。

   请在流行为视图下执行命令 **statistic enable** 开启流策略统计功能。执行 **display traffic policy statistics** 查看是否有流量统计。

   - 如果显示为没有流量统计，说明报文没有命中流策略，请按照 **9.1 流策略故障处理**排除流策略的故障。
   - 如果已经有流量统计，请执行步骤 3。

步骤 3 检查观察接口是否有报文发出

执行 **display interface** 命令查看观察接口的信息，“Output”为观察接口发出的报文信息。

- 如果观察接口发出的报文的统计信息为 0 或者不变化，观察接口没有发出报文，请根据实际情况选择执行以下部分。

  1. 执行 **display interface** 检查接口状态是否为“Up”，如果状态为“Down”，请解决链路故障。如果接口状态为“Up”，请执行步骤 b。
  2. 检查配置流行为时指定的观察接口的索引是否与已创建的观察接口的索引相同，如果不相同，请在流行为视图下执行命令 **mirror（流行为视图）**将满足规则的流镜像到已经创建的观察接口。如果相同，请执行步骤 4。

- 如果观察接口发出的报文的统计信息不为 0 且不断不变化，说明观察接口发出了报文，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

2.4.3 故障案例

介绍了端口镜像和流镜像的实际处理案例。

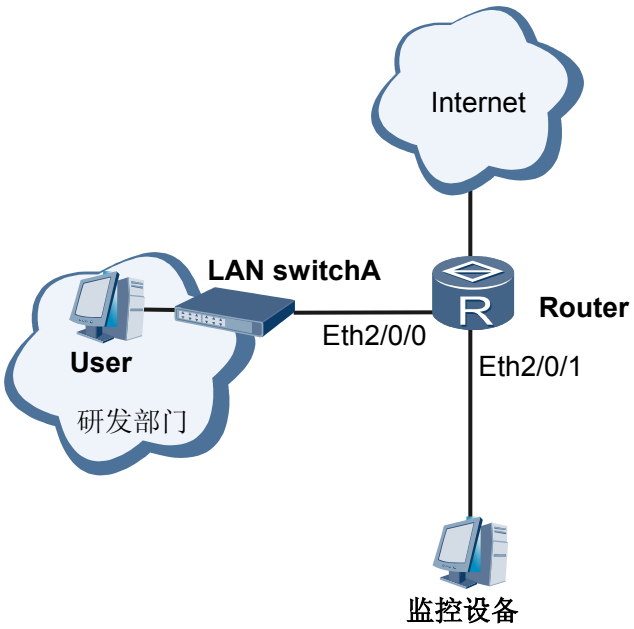
监控设备看不到端口镜像报文

网络环境

如图 2-6 所示，研发部门通过 Router 访问 Internet。

监控设备为实现对研发部门访问 Internet 的流量分析，在 Router 上配置端口镜像，Eth2/0/0 作为镜像端口，Eth2/0/1 作为观察端口。配置完成后，发现当研发部门访问 Internet 时，监控设备上无法看到镜像报文。

图 2-6 监控设备看不到端口镜像报文组网图



故障分析

1. 执行 **display interface** 命令，检查镜像端口 Eth2/0/0 是否接收到用户发来的报文。

   命令行的输出信息中“Input”信息不为“0”且不断累加，镜像端口接收到了用户发送至 Internet 的报文。

2. 检查镜像接口配置是否正确

   执行 **display mirror-port** 命令，输出信息中“Mirror-port”为 Eth2/0/0，“Observe-port”为 Eth2/0/3。观察接口配置不正确。

操作步骤

步骤 1 在 RouterA 上执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行 **observe-port interface ethernet** 2/0/1 ，配置本地观察端口为 Ethernet 2/0/1。

步骤 3 执行 **interface ethernet** 2/0/0，进入镜像接口视图。

步骤 4 执行 **mirror to observe-port inbound**，配置镜像功能。

----结束

案例总结

观察接口与镜像接口的对应关系配置错误会导致监控设备看不到端口镜像报文。

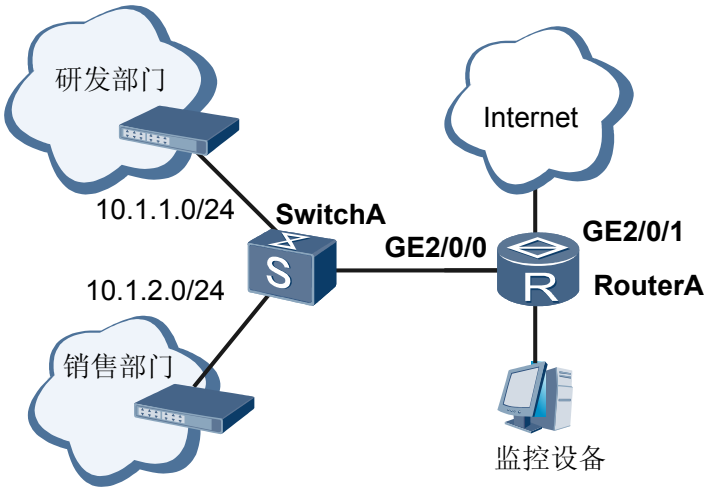
监控设备看不到流镜像报文

网络环境

如图 2-7 所示，某公司的研发部门，销售部门和 IT 部门位于不同的网段。

研发部门和市场部门通过 RouterA 访问 Internet。IT 部门在 RouterA 上配置了流镜像对研发部门访问 Internet 的流量进行分析。配置完成后，监控设备上无法观测到镜像报文。

图 2-7 监控设备看不到端口镜像报文组网图



故障分析

1. 执行 **display interface** 命令，检查镜像端口 GigabitEthernet2/0/0 是否接收到用户发来的报文。

   输出信息中“Input”信息不为“0”且不断累加，镜像端口接收到了用户网络发送的报文。

2. 检查流策略是否被应用

   执行命令 **display traffic-policy** *policy-name* **apllied-record** 查看流策略的应用记录。显示信息中显示流策略 **tp1** 已经在接口 GigabitEthernet2/0/0 下应用。

3. 检查报文是否命中流策略

版权所有 © 华为技术有限公司

在流行为视图下执行命令 **statistic enable** 命令使能流策略的流量统计功能，执行命令 **display traffic policy statistics interface GigabitEthernet 2/0/0 inbound** 发现流策略接收和统计数据均为零。报文没有命中流策略。

4. 检查流策略中的流分类和流行为是否正确。

   执行命令 **display traffic policy user-defined** 检查流策略中是否绑定了带有流镜像动作的流行为。

```
<Huawei> display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: default-class
     Behavior: be
      -none-
   Classifier: tc1
     Behavior: tb1
      statistic: enable
      Port-mirroring  to observe-port 1
```

   显示信息表明，流策略中配置绑定了流分类 **tc1** 和流行为 **tb1**，流行为 **tb1** 中配置了正确的流镜像动作。请执行命令 **display traffic classifier user-defined** 检查流分类配置是否正确，如果流分类中配置 ACL，还要执行命令 **display acl** 进一步检查 ACL 规则的正确性。

```
<Huawei> display traffic classifier user-defined tc1
  User Defined Classifier Information:
   Classifier: tc1
    Precedence: 10
    Operator: AND
    Rule(s) : if-match acl 3000
              if-match inbound-interface GigabitEthernet 1/0/0
<Quidqway> display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255
```

   显示信息表明，流分类的匹配规则为匹配 ACL 3000 和入接口 GigabitEthernet1/0/0，规则间逻辑关系为“AND”。如果流分类规则间的逻辑关系为“AND”，则报文必须匹配流分类中所有的非 ACL 规则和其中一条 ACL 规则才能命中。由于报文入接口为 GigabitEthernet2/0/0 而不是 GigabitEthernet1/0/0，因此报文没有命中流策略，导致监控设备看不到用户的报文。

操作步骤

步骤 1 执行 **interface GigabitEthernet 2/0/0** 命令进入镜像接口视图。

步骤 2 执行命令 **undo traffic-policy inbound**，取消流策略在接口的应用。

步骤 3 执行命令 **quit**，退出接口视图。

步骤 4 执行命令 **traffic classifier tc1**，进入流分类视图。

步骤 5 执行命令 **undo if-match inbound-interface**，删除原有的基于入接口对报文进行流分类的匹配规则。

步骤 6 执行命令 **if-match inbound-interface GigabitEthernet 2/0/0**，重新配置基于入接口 GigabitEthernet2/0/0 对报文进行流分类的匹配规则。

步骤 7 执行命令 **quit**，退出流分类视图。

步骤 8 执行命令 **interface GigabitEthernet 2/0/0** 进入接口视图。

步骤 9 执行命令 **traffic-policy tp1 inbound**，将流策略应用在接口下。

----结束

版权所有 © 华为技术有限公司

案例总结

在配置流镜像时，需要注意定义的流策略是否正确，不能命中流策略的报文将不会被复制到观察接口。

2.5 SNMP 故障处理

2.5.1 SNMP 无法连接的定位思路

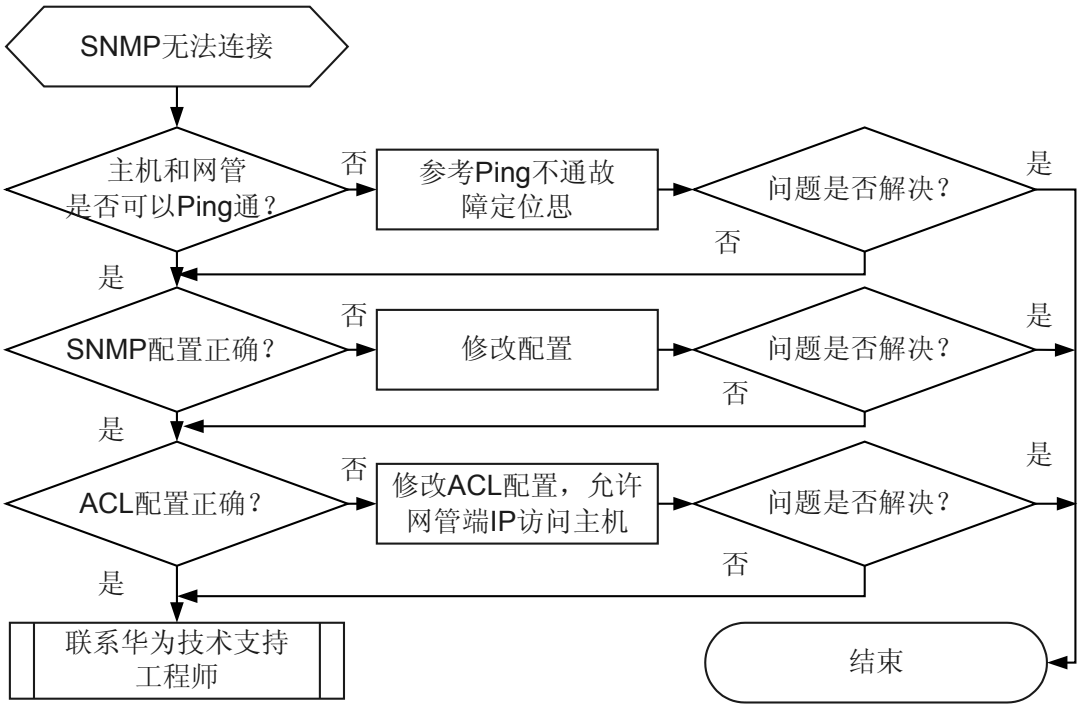
常见原因

本类故障的常见原因主要包括：

- 报文不可达造成无法连接。
- 配置原因造成无法连接。

故障诊断流程

图 2-8 SNMP 无法连接诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 执行 **ping** 命令查看主机和网管之间是否可以 Ping 通。

- 如果无法 Ping 通，请参见 **Ping 不通问题**继续定位，使主机和网管之间可以 Ping 通。
- 如果可以 Ping 通，说明主机和网管之间有可达的路由，则执行步骤 2。

步骤 2 检查主机的 SNMP 配置是否正确。

- 如果配置不正确，请参见**表 2-1** 修改配置。
- 如果配置正确，请执行步骤 3。

表 2-1 SNMP 配置

检查项	检查方法	处理步骤
查看主机是否支持网管发送登录请求所使用的 SNMP 协议版本。	执行 **display snmp-agent sys-info version** 命令查看主机配置的 SNMP 版本。	如果主机配置的 SNMP 版本非网管所使用的版本，请执行 **snmp-agent sys-info version** 命令修改主机的 SNMP 版本。
查看主机配置的团体字。	执行 **display snmp-agent community** 命令查看。	如果网管发起请求时使用的团体字和主机配置的团体字不相同，请执行 **snmp-agent community** 命令修改主机的读写团体名，使之与网管端配置一致。
对于 SNMPv3，同时查看 SNMP 用户组和用户信息配置是否正确。	• 执行 **display snmp-agent group** 命令查看 SNMPv3 用户组信息。 • 执行 **display snmp-agent usm-user** 命令查看 SNMPv3 用户信息。	如果配置不正确，请重新配置。 • 执行 **snmp-agent group** 命令配置 SNMPv3 用户组信息。 • 执行 **snmp-agent usm-user** 命令配置 SNMPv3 用户信息。

步骤 3 执行 **display acl** 命令查看主机 ACL 配置。

- 如果网管端发送请求所使用的 IP 被 ACL 禁止访问，请执行 **rule** 命令配置允许网管端 IP 访问主机。
- 如果网管端发送请求所使用的 IP 未被 ACL 禁止访问，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警与日志

相关告警

无

相关日志

无

2.5.2 网管无法收到主机发送的告警的定位思路

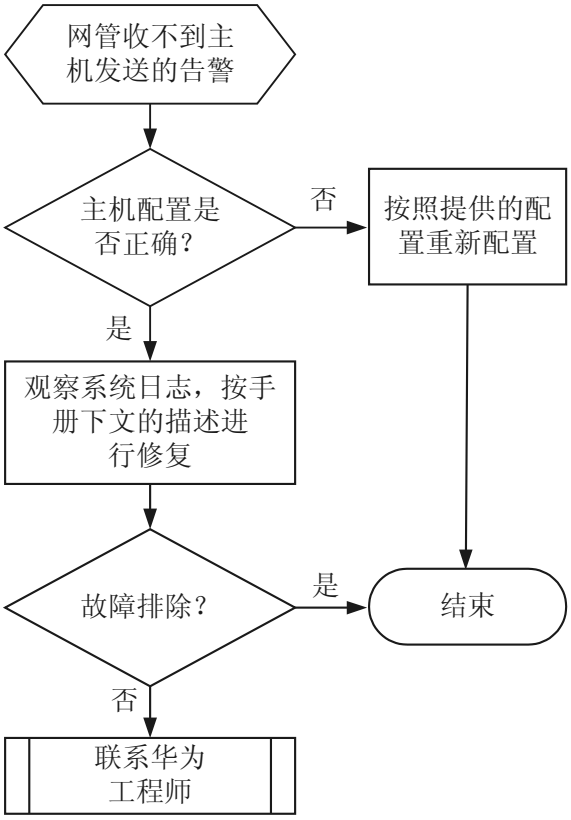
常见原因

本类故障的常见原因主要包括：

- 报文丢失造成网管主机无法接收到这条告警。
- 主机侧 SNMP 配置错误，造成告警无法发送。
- 主机侧业务模块没有产生告警，或者产生的告警格式错误导致告警无法发送。

故障诊断流程

图 2-9 网管收不到主机告警的诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查设备上 Trap 目的主机的配置是否正确。

- 如果 Trap 主机配置正确，则执行步骤 2。
- 如果 Trap 主机配置错误，可以参考如下配置案例进行修改：

表 2-2 Trap 主机典型配置

配置例	命令行
配置一个版本为 SNMPv2c 的 Trap 主机，不携带 VPN，端口号为默认值 162，安全名为 huawei，IP 地址为 192.168.1.1	<Huawei> **system-view** [Huawei] **snmp-agent target-host trap-paramsname abc v2c securityname huawei** [Huawei] **snmp-agent target-host trap-hostname aaa address 192.168.1.1 trap-paramsnam abc**
配置一个 SNMPv3 用户，用户名为 huawei，属于一个叫做 huawei_group 的用户组，拥有的告警权限（Notify－view）是 Huawei_view，Huawei_view 的权限是从 iso 子树开始的节点全部可以访问	# 配置 MIB 视图。 <Huawei> **system-view** [Huawei] **snmp-agent mib-view Huawei_view include iso** # 配置用户组。 [Huawei] **snmp-agent group v3 huawei_group noauth read-view Huawei_view write-view Huawei_view notify-view Huawei_view** # 配置用户。 [Huawei] **snmp-agent usm-user v3 huawei huawei_group**
配置一个版本为 V3 的 Trap 主机，不携带 VPN，端口号为默认值 162，用户名为 huawei，IP 地址为 192.168.1.1（huawei 必须是一个确实存在的用户）	<Huawei> **system-view** [Huawei] **snmp-agent target-host trap-paramsname abc v3 securityname huawei authentication** [Huawei] **snmp-agent target-host trap-hostname aaa address 192.168.1.1 trap-paramsname abc**

步骤 2 执行 **display snmp-agent trap all** 命令可以查看到的告警的使能情况。

- 如果告警没有使能，则执行 **snmp-agent trap enable** 命令使能设备对网管发送 Trap 报文的功能。
- 如果告警已经使能，则执行步骤 3。

步骤 3 获取主机上的日志，检查是否有告警产生的信息。

- 如果没有期望获取的告警的记录，说明告警没有产生，请执行步骤 4。
- 如果存在期望获取的告警的记录，说明告警已经产生但是网管没有收到，请执行步骤 4。

版权所有 © 华为技术有限公司

说明

观察日志中是否有告警产生的信息，类似如下形式：
#Jun 10 2010 09:55:03 Quideway IFNET/2/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Interface 109 turned into DOWN state.

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.6 RMON 故障处理

2.6.1 网管无法接收 RMON 告警信息的定位思路

常见原因

本类故障的常见原因主要包括：

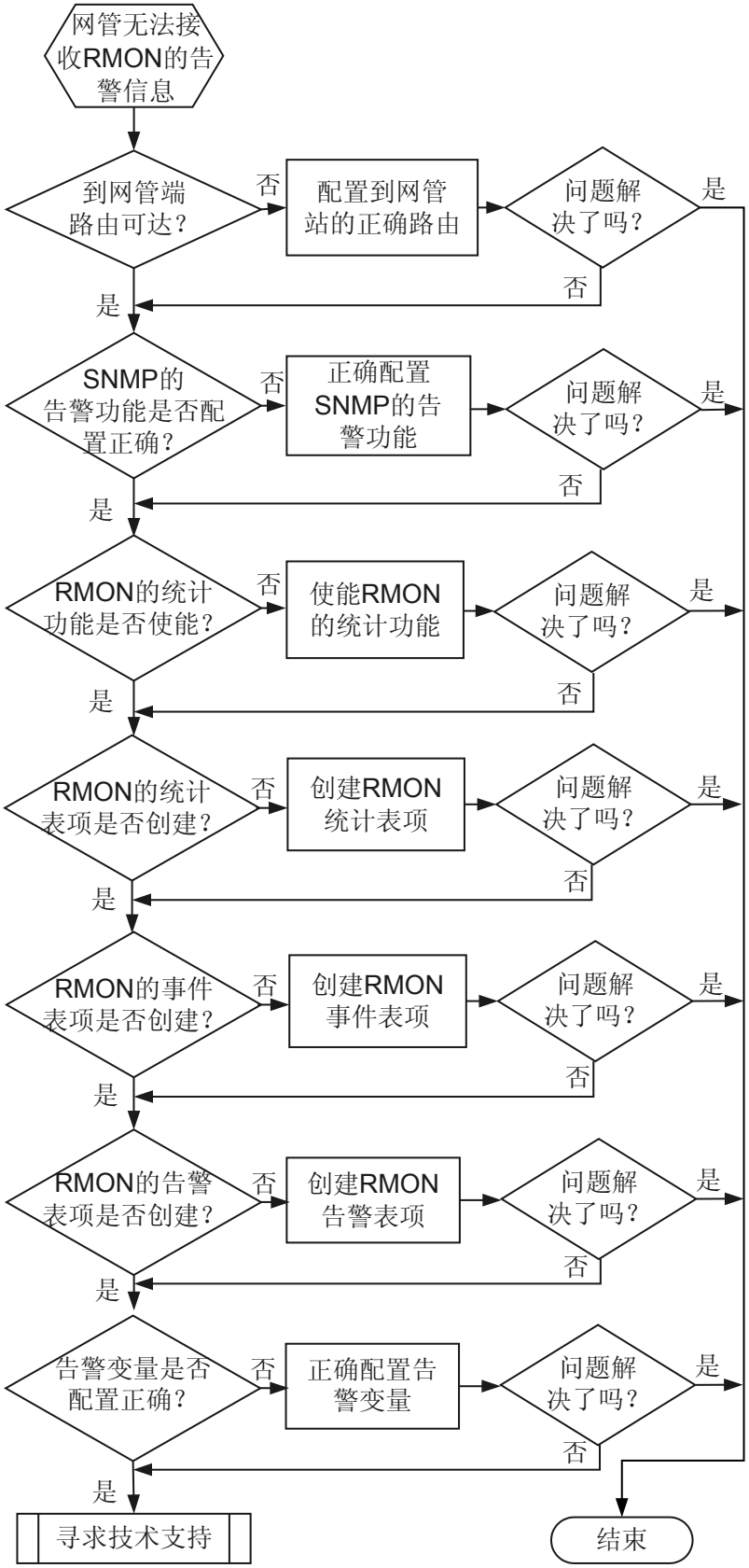
- 设备到网管端之间的路由不可达。
- SNMP 告警功能配置错误。
- RMON 统计表未配置。
- RMON 统计功能未使能。
- RMON 的事件表未使能。
- RMON 的告警表未使能。
- 告警变量配置错误。

故障诊断流程

在流入、流出局域网的流量超过配置的阈值时，网管没有得到告警信息。请使用下面的故障诊断流程，如图 2-10 所示。

版权所有 © 华为技术有限公司

图 2-10 网管无法接收 RMON 告警信息故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查路由器到网管端是否路由可达

在路由器端 Ping 网管端是否可以 Ping 通。

- 如果可以 Ping 通说明路由器和网管端的路由可达，则执行步骤 2。
- 如果 Ping 不通，请检测路由器和网管端的路由，请参见 **Ping 不通问题**。

步骤 2 检查 SNMP 告警功能是否配置正确

在网管端检查是否可以接收到其他的告警信息，如无法接收到其他的告警信息。

- 执行命令 **display snmp-agent trap all**，检查路由器的告警功能是否已经使能。
- 执行命令 **display snmp-agent target-host**，检查路由器配置发送告警的网管地址是否正确。

步骤 3 检查是否使能了 RMON 统计功能

在相应的端口下执行命令 **display this**，查看端口的 RMON 统计功能是否使能。如果端口下没有使能 RMON 统计功能，请在端口下执行 **rmon-statistics enable**。

步骤 4 检查是否配置了 RMON 统计表

在路由器端执行命令 **display rmon statistics**，查看是否配置了 RMON 统计表。如果统计表为空，请使用命令 **rmon statistics** *entry-number* [**owner** *owner-name*]创建统计表表项。

步骤 5 检查是否使能 RMON 的事件表

在路由器端执行命令 **display rmon event** [*entry-number*]，查看 RMON 的事件表是否使能。如果事件表为空，请使用命令 **rmon event** 创建事件表表项。

步骤 6 检查是否使能 RMON 的告警表

在路由器端执行命令 **display rmon alarm** [*entry-number*]，查看 RMON 的告警表是否使能。如果告警表为空，请使用命令 **rmon alarm** 创建告警表表项。

步骤 7 检查告警变量的配置是否正确

在路由器端执行命令 **display rmon alarm** [*entry-number*]，查看配置的告警变量的值。在网管端查看需要监控的接口的告警变量的值是否和路由器端配置的一致，如果不一致，请修改告警变量的值。

步骤 8 如果经过上述的检查步骤，网管端仍然无法接收到路由器 RMON 模块的告警值，请收集如下信息，联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警与日志

相关告警

无

相关日志

无

2.7 NQA 故障处理

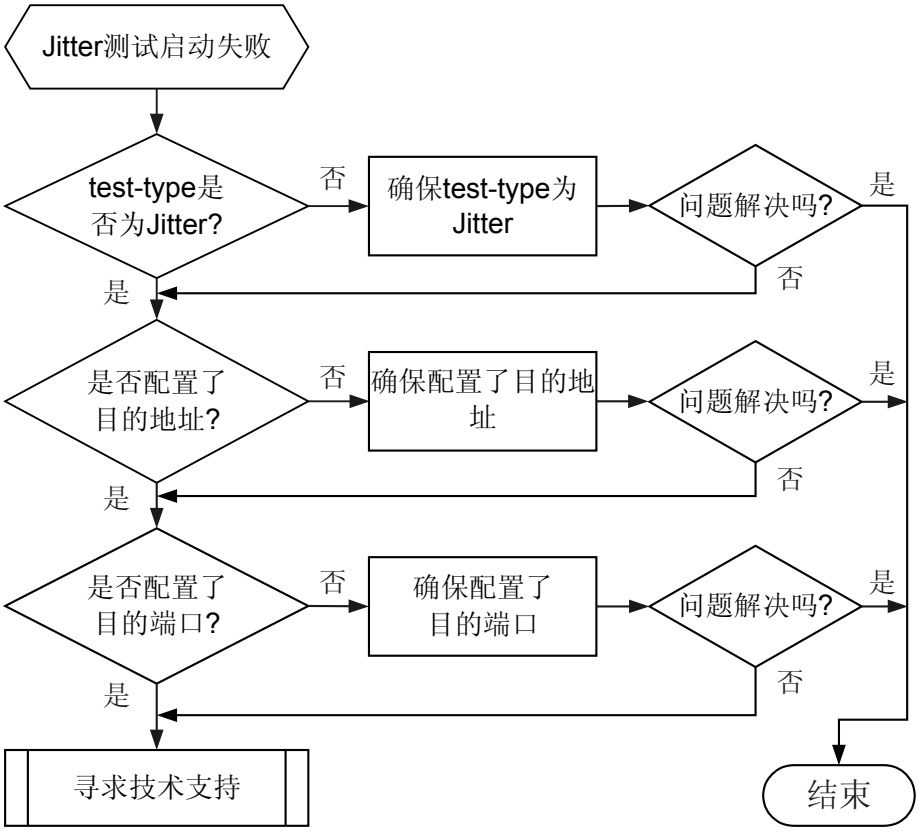
2.7.1 无法启动 UDP Jitter 测试的定位思路

常见原因

本类故障的常见原因是：测试例必配参数配置错误。

故障诊断流程

图 2-11 UDP Jitter 测试无法启动故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

除 display 命令可以在所有视图下执行外，以下命令如无特殊说明，都是在 NQA 测试例视图下执行。

操作步骤

步骤 1 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]，或者在 NQA 测试例视图下执行命令 **display this**，查看测试例类型是否配置为 jitter。

- 如果是，请执行步骤 2。
- 如果否，请执行命令 **test-type jitter**，配置测试例类型为 UDP Jitter。
  - 如果问题解决，结束操作。
  - 如果问题未解决，请执行步骤 2。

步骤 2 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]，或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了目的地址。

- 如果是，请执行步骤 3。
- 如果否，请执行命令 **destination-address ipv4** *ip-address*，配置目的地址。
  - 如果问题解决，结束操作。
  - 如果问题未解决，请执行步骤 3。

步骤 3 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]，或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了目的端口。

- 如果是，请执行步骤 4。
- 如果否，请执行命令 **destination-port** *port-number*，配置目的端口号。
  - 如果问题解决，结束操作。
  - 如果问题未解决，请执行步骤 4。

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.7.2 UDP Jitter 测试结果有 drop 记录的定位思路

版权所有 © 华为技术有限公司

常见原因

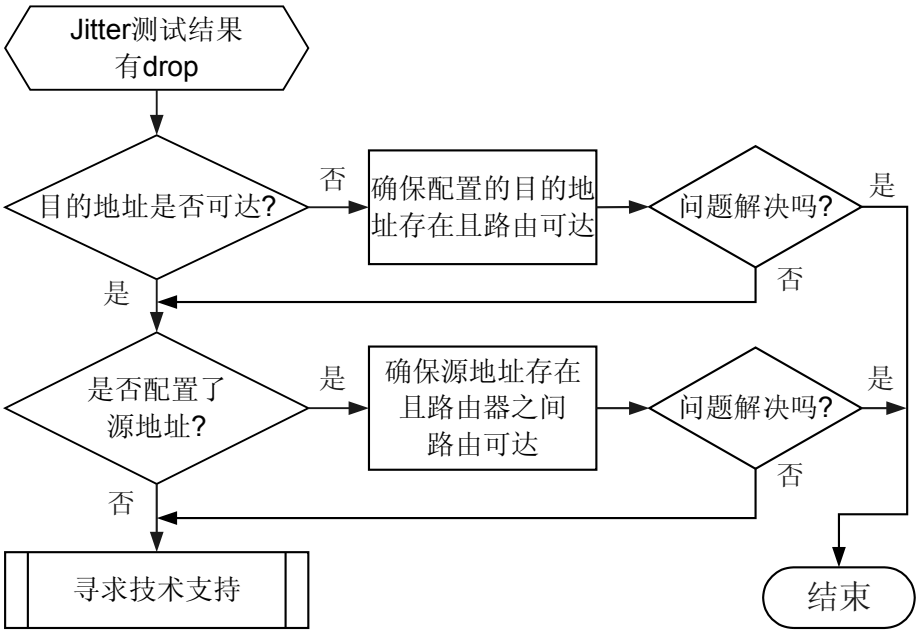
UDP Jitter 测试结果有 drop 记录是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时，显示信息中“Drop operation number”字段的值不是 0。

本类故障的常见原因是：

- 目的地址不存在或路由表项中没有该网段路由。
- 源地址配置错误。

故障诊断流程

图 2-12 UDP Jitter 测试结果有 drop 记录的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 在 NQA 测试客户端上执行命令 **display ip routing-table**，查看到服务器的单播路由是否存在。

- 如果存在，执行命令 **ping** 检查路由是否可达。
  - 如果路由可达，请执行步骤 2。
  - 如果路由不可达，请参见 **Ping 不通问题**。
- 如果不存在，请执行相应的路由配置命令，重新配置路由。

步骤 2 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]，或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了源地址。

版权所有 © 华为技术有限公司

- 如果是，在 NQA 客户端执行 **display ip interface brief** 命令查看是否存在配置了该源地址的接口。
  - 如果是，在 NQA 服务器端执行命令 **display ip routing-table** 查看到客户端的单播路由是否存在。
    - 如果存在，执行命令 **ping** 检查路由是否可达。
      - 如果路由可达，请执行步骤 3。
      - 如果路由不可达，请参见 **Ping 不通问题**。
    - 如果不存在，请执行相应的路由配置命令，重新配置路由。
  - 如果否，请重新分配接口的 IP 地址并检查 NQA 配置。
- 如果否，请执行步骤 3。

步骤 3 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.7.3 UDP Jitter 测试结果有 busy 记录的定位思路

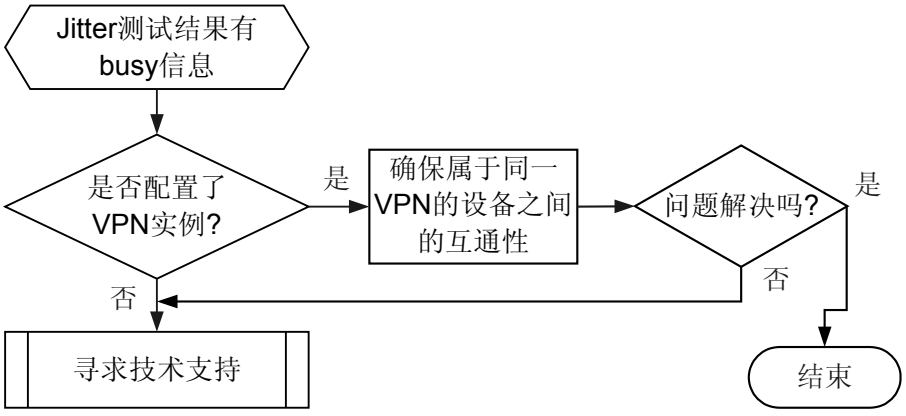
常见原因

UDP Jitter 测试结果有 busy 记录是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时，显示信息中“System busy operation number”字段的值不是 0。

本类故障的常见原因是测试例配置的 VPN 实例路由不可达。

故障诊断流程

图 2-13 UDP Jitter 测试结果有 busy 记录的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]，或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了 VPN 实例。

- 如果是，请执行步骤 2。
- 如果否，请执行步骤 3。

步骤 2 在 NQA 客户端上执行命令 **ping -vpn-instance** *vpn-instance-name*，查看目的地址是否可达。

- 如果是，请执行步骤 3。
- 如果否，请参见 **Ping 不通问题**。

步骤 3 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.7.4 UDP Jitter 测试结果有 timeout 记录的定位思路

常见原因

UDP Jitter 测试结果有 timeout 记录是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时，显示信息中“Operation timeout number”字段的值不是 0。

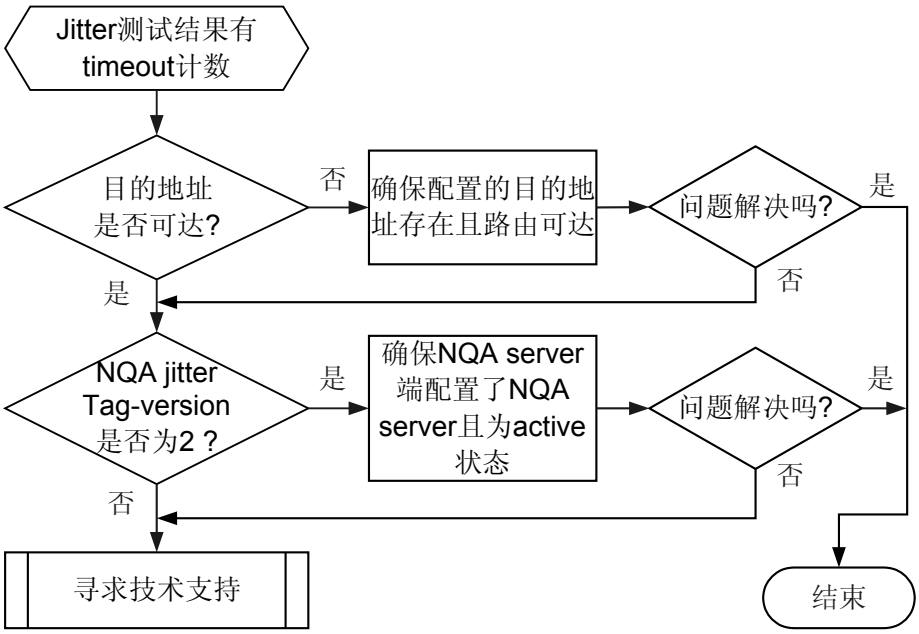
本类故障的常见原因：

- 目的地址不存在但路由表项中可以看到该网段路由
- nqa-jitter tag-version 值为 2，且接收端没有配置 UDP Server

版权所有 © 华为技术有限公司

故障诊断流程

图 2-14 UDP Jitter 测试结果有 timeout 记录的故障诊断流程图



故障处理步骤

说明

请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。

除 display 命令可以在所有视图下执行外，以下命令如无特殊说明，都是在 NQA 测试例视图下执行。

操作步骤

步骤 1 在 NQA 客户端上执行 **ping** 命令，检查到目的端的路由是否可达。

- 如果是，请执行步骤 2。
- 如果否，请参见 **Ping 不通问题**。

步骤 2 在 NQA 客户端上系统视图下执行命令 **display this**，查看配置的 **nqa-jitter tag-version** 是否为 2（当该参数配置为 1 时，即为默认值时，配置文件中不显示，配置为 2 时显示）。

- 如果是，请执行步骤 3。
- 如果否，请执行步骤 4。

步骤 3 在服务器端执行命令 **display nqa-server**，查看 NQA 服务器端是否存在 **nqa-server udpecho** *ip-address port-number* 配置。

- 如果是且为 active 状态，请执行步骤 4。
- 如果否，请在服务器端上使用命令 **nqa-server udpecho** *ip-address port-number* 配置 NQA 服务器。其中，*ip-address* 需要与客户端 **destination-address ipv4** *ip-address* 命令配置的一致；*port-number* 需要与客户端 **destination-port** *port-number* 配置的一致。

版权所有 © 华为技术有限公司

- 如果问题解决，结束操作。
- 如果问题未解决，请执行步骤 4。

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.7.5 UDP Jitter 测试结果 failed、no result 或者有丢包的定位思路

常见原因

UDP Jitter 测试结果 failed、no result 或者有丢包是指使用 **display nqa results** 命令查看 NQA 测试的结果统计时：

- 如果显示信息中“Completion”字段的值为“failed”，说明测试结果失败。
- 显示信息中“Completion”字段的值为“no result”，说明测试没有得到结果。
- 显示信息中“Lost packet ratio”字段的值不是 0%，说明有丢包。

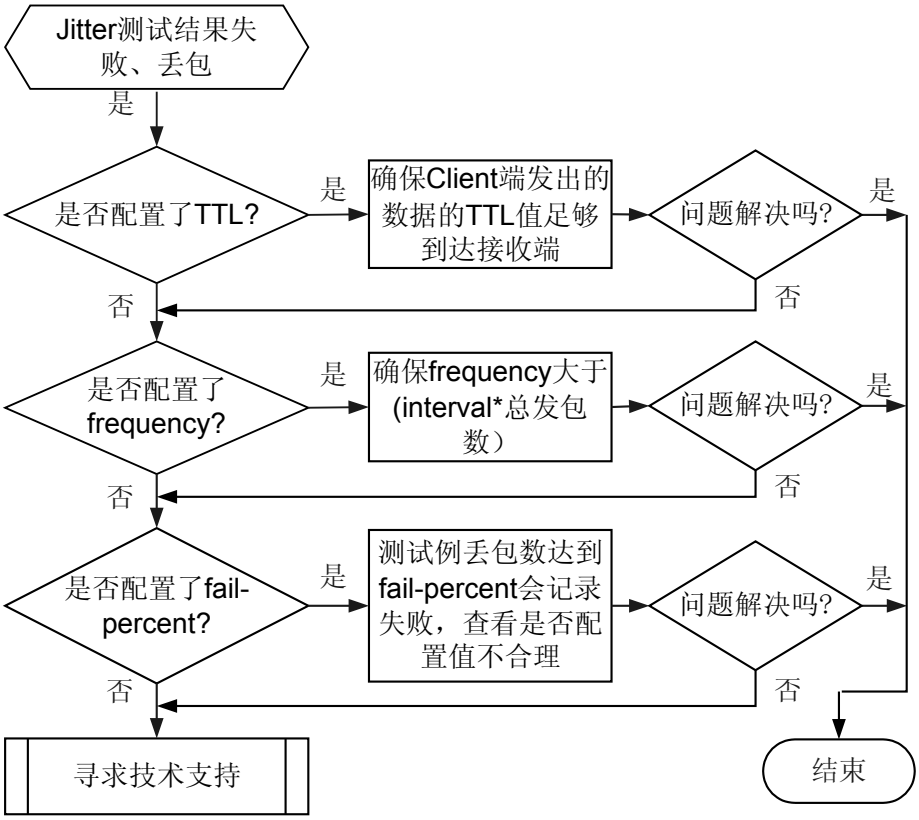
本类故障的常见原因是：

- UDP Jitter 测试结果有 drop 计数
- UDP Jitter 测试结果有 busy 计数
- UDP Jitter 测试结果有 timeout 计数
- TTL 超时
- frequency 配置错误
- fail-percent 配置错误

版权所有 © 华为技术有限公司

故障诊断流程

图 2-15 UDP Jitter 测试结果 failed、no result 或者有丢包的故障诊断流程图



故障处理步骤

说明

请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。

除 display 命令可以在所有视图下执行外，以下命令如无特殊说明，都是在 NQA 测试例视图下执行。

操作步骤

步骤 1 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了 ttl 参数。

- 如果配置了 TTL，请使用 **ttl number** 将 TTL 设置为 255，如果设置为 255 后故障还是存在，请执行步骤 2。
- 如果没有配置 TTL，请使用 **ttl number** 将 TTL 设置为 255，如果设置为 255 后故障还是存在，请执行步骤 2。

步骤 2 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了 frequency 参数。

- 如果是，比较（interval * probe-count*jitter-packetnum）与 frequency 的大小，如果（interval*probe-count*jitter-packetnum）大于 frequency，请使用命令 **frequency**

版权所有 © 华为技术有限公司

interval 增大 frequency 值。frequency 必须大于（interval*probe-count*jitter-packetnum），才能保证测试例正常结束。

- 如果没有配置 frequency 或配置了合理的 frequency 后故障仍然存在，请执行步骤 3。

步骤 3 在 NQA 客户端上执行命令 **display nqa-agent** *admin-name test-name* [**verbose**]或者在 NQA 测试例视图下执行命令 **display this**，查看是否配置了 fail-percent 参数。

- 如果配置了 fail-percent 参数，请使用命令 **undo fail-percent** 将 fail-percent 参数配置取消。如果 fail-percent 参数取消后故障仍然存在，请执行步骤 4。
- 如果没有配置 fail-percent 参数，请执行步骤 4。

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

2.8 NTP 故障诊断思路

2.8.1 时钟未同步的定位思路

常见原因

- 链路震荡
- 链路不通

故障处理步骤

说明

请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。

操作步骤

步骤 1 查看 NTP 状态。

```
<Huawei> display ntp-service status
 clock status: unsynchronized
 clock stratum: 16
 reference clock ID: none
 nominal frequency: 100.0000 Hz
 actual frequency: 99.9995 Hz
 clock precision: 2^18
 clock offset: 0.0000 ms
```


版权所有 © 华为技术有限公司

```
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 0.00 ms
reference time: 14:25:55.477 UTC Jun 9 2010(CFBA22F3.7A4B76F6)
```

“clock status”字段为 unsynchronized 说明本地时钟未被同步到任何一个 NTP 服务器或时钟源。

步骤 2 查看 NTP 连接状态。

```
<Huawei> display ntp-service sessions
```

“reference”为 0.0.0.0 说明本地时钟未同步到任何一个 NTP 服务器。

步骤 3 在 NTP 客户端执行命令 **ping** 检查到服务器端的链路状态。例如：

```
<Huawei> ping 20.1.14.1
  PING 20.1.14.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
  --- 20.1.14.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

- **“100.00% packet loss”**说明链路不通，请参见 **Ping 不通问题**继续定位问题。
- 如果不是 100.00%，说明链路震荡，请参见 **Ping 不通问题**继续定位问题。
- 如果是 0.00%，说明链路没有问题，请执行步骤 4。

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

以下日志说明本地同步的时钟源丢失：

NTP/4/SOURCE_LOST

以下日志说明本地同步到某个时钟源：

NTP/4/LEAP_CHANGE
NTP/4/STRATUM_CHANGE
NTP/4/PEER_SELE

2.9 CWMP 故障处理

版权所有 © 华为技术有限公司

2.9.1 通过 CWMP 管理设备失败的定位思路

常见原因

通过 CWMP 管理设备失败，包括两种情况：

- 设备无法与 ACS 建立连接。
- ACS 下发操作执行失败。

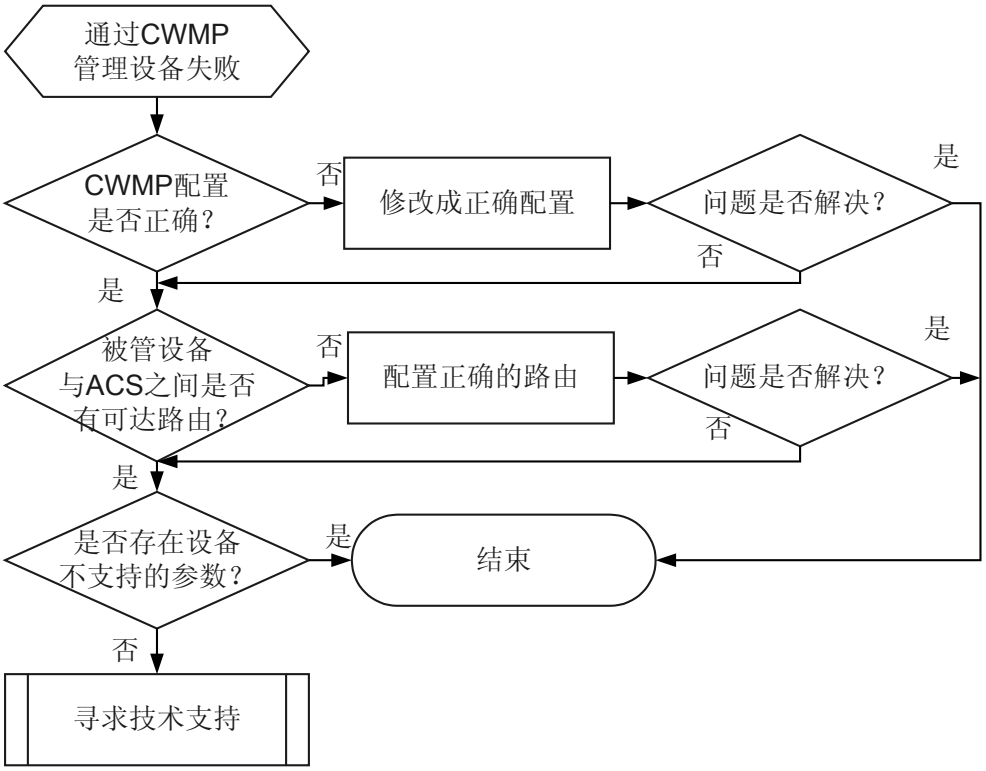
本类故障的常见原因主要包括：

- 设备上 CWMP 的相关配置错误，包括 ACS URL、用户名、密码、CWMP 未使能等。
- 设备与 ACS 之间无可达路由。
- 设备不支持 ACS 下发的部分或全部参数。

故障诊断流程

详细处理流程如图 2-16 所示。

图 2-16 通过 CWMP 管理设备失败故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查设备上 CWMP 配置是否正确。

在系统视图下执行 **display cwmp configuration** 命令，查看 CWMP 状态是否使能、ACS 的 URL、用户名和密码配置是否正确。

```
<Huawei> display cwmp configuration
  CWMP is enabled
  ACS URL:                        http://www.acs.com:80/acs
  ACS username:                   hwcpe
  ACS password:                   %$%$gwl.QU~4M1I@RDF>b/VP,@7.%$%$
  Inform enable status:                disabled
  Inform interval:                     600s
  Inform time:                         -
  Wait timeout:                        30s
  Reconnection times:                  3
```

- 如果配置正确，请执行步骤 2。
- 如果配置不正确，请参照表 2-3 修改配置，然后执行命令 **undo cwmp enable** 和 **cwmp enable** 重启 CWMP 功能。

表 2-3 配置 CWMP 功能

配置项	配置方法
使能 CWMP 功能	在 CWMP 视图下执行命令 **cwmp enable**
配置设备连接到 ACS 的 URL	在 CWMP 视图下执行命令 **cwmp acs url** *url*
配置设备连接到 ACS 的用户名	在 CWMP 视图下执行命令 **cwmp acs username** *username*
配置设备连接到 ACS 的密码	在 CWMP 视图下执行命令 **cwmp acs password cipher** *password*

步骤 2 检查设备与 ACS 之间是否有可达路由。

在设备上执行 **ping** 命令，查看是否可以 Ping 通 ACS。

说明

如果配置的 ACS 的 URL 是域名，则可以通过 **display dns dynamic-host** 命令获取到域名解析后的 IP 地址，然后执行 Ping 命令。

```
<Huawei> display dns dynamic-host
  No  Domain-name          IpAddress            TTL      Alias
  1   huawei.com           2.1.1.3              3579
```

- 如果 Ping 不通，请参见 7.1.1 Ping 不通问题的定位思路继续定位，使设备能 Ping 通 ACS。
- 如果能够 Ping 通，请执行步骤 3。

步骤 3 检查 ACS 下发的报文中的参数是否是 AR 支持的参数。

通过 Ethereal 或者其他抓包工具抓取 ACS 和 AR 设备的交互报文，查看报文中的参数，即<Name></Name>字段中的值。

版权所有 © 华为技术有限公司

```
<soapenv:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsd="http://www.w3.org/2
    <soapenv:Header>
        <cwmp:ID soapenv:mustUnderstand="1">null0</cwmp:ID>
    </soapenv:Header>
    <soapenv:Body>
        <cwmp:SetParameterValues>
            <ParameterList soap:arrayType="cwmp:ParameterValueStruct[4]">
                <ParameterValueStruct>
                    <Name>InternetGatewayDevice.ManagementServer.PeriodicInformEnable</Name>
                    <Value xsi:type="xsd:boolean">1</Value>
                </ParameterValueStruct>
                <ParameterValueStruct>
                    <Name>InternetGatewayDevice.ManagementServer.ConnectionRequestUsername</Name>
                    <Value xsi:type="xsd:string">001803-AR1220-1200201009080001</Value>
                </ParameterValueStruct>
                <ParameterValueStruct>
                    <Name>InternetGatewayDevice.ManagementServer.ConnectionRequestPassword</Name>
                    <Value xsi:type="xsd:string">b74f97f107c1448ea5cb134f28d27435</Value>
                </ParameterValueStruct>
                <ParameterValueStruct>
                    <Name>InternetGatewayDevice.ManagementServer.PeriodicInformInterval</Name>
                    <Value xsi:type="xsd:unsignedInt">120</Value>
                </ParameterValueStruct>
            </ParameterList>
            <ParameterKey>null</ParameterKey>
        </cwmp:SetParameterValues>
    </soapenv:Body>
</soapenv:Envelope>
```

- 如果有设备不支持的参数，会导致 ACS 管理设备失败。
- 如果没有设备不支持的参数，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

3 物理对接及接口类

关于本章

3.1 Eth-Trunk 接口故障处理
介绍了 Eth-Trunk 接口常见故障原因的定位思路和案例。

华为专有和保密信息
版权所有 © 华为技术有限公司

3.1 Eth-Trunk 接口故障处理

介绍了 Eth-Trunk 接口常见故障原因的定位思路和案例。

3.1.1 Eth-Trunk 转发不通的定位思路

介绍 Eth-Trunk 转发不通的故障原因、处理流程和详细的故障处理步骤。

常见原因

配置 Eth-Trunk 接口后，Eth-Trunk 接口无法正常转发流量。

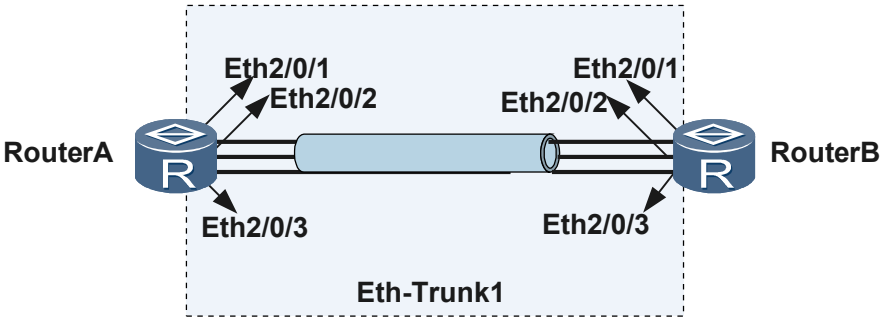
本类故障的常见原因有：

- Eth-Trunk 接口成员口故障。
- 设备两端的 Eth-Trunk 接口成员口配置不一致。
- 状态为 Up 的 Eth-Trunk 接口的成员口数量小于配置的下限阈值。
- 静态 LACP 模式的 Eth-Trunk 接口成员口协商不成功。

故障诊断流程

如图 3-1 所示，Eth-Trunk 接口转发不通的故障处理将基于该网络。

图 3-1 Eth-Trunk 接口组网图



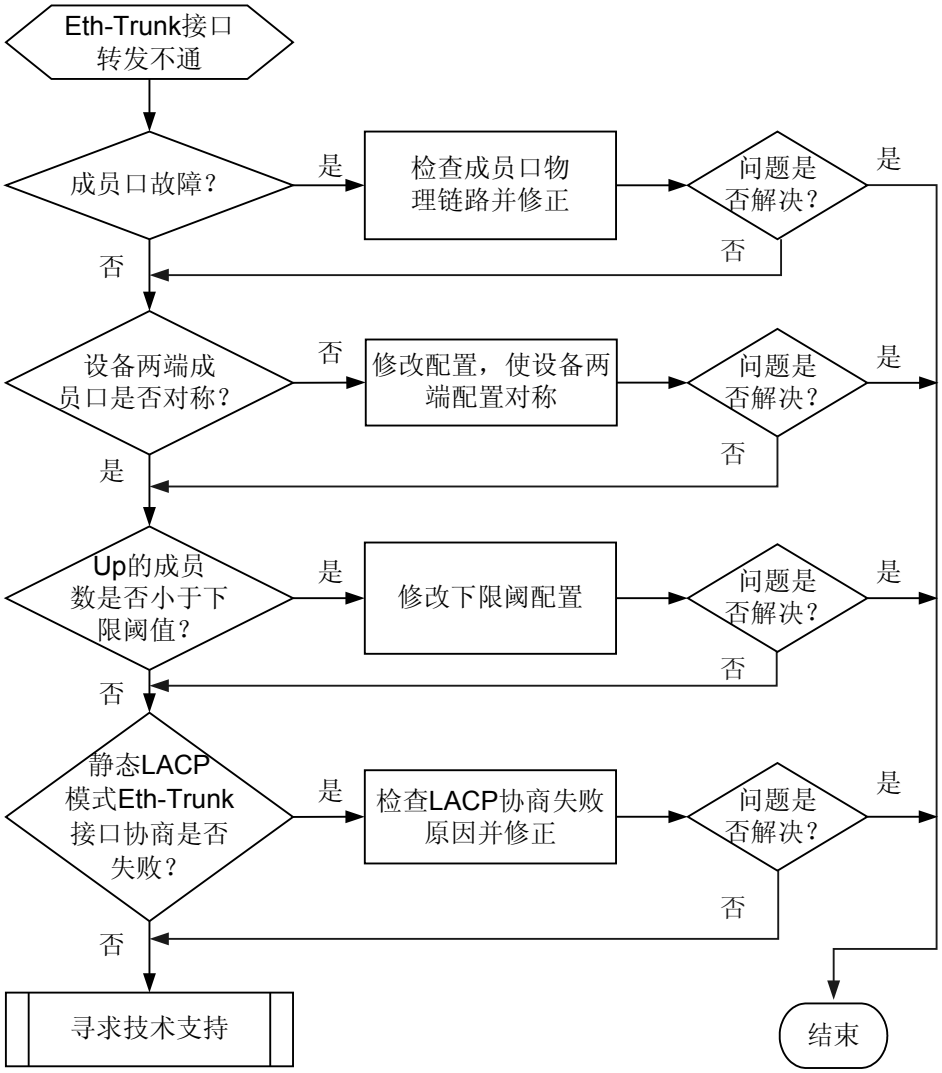
故障诊断思路：

- 检查 Eth-Trunk 接口成员口是否存在故障。
- 检查设备两端 Eth-Trunk 接口的成员口信息。
- 检查状态为 Up 的成员口数是否小于配置的下限阈值。
- 若 Eth-Trunk 接口是静态 LACP 模式，检查 LACP 是否协商成功。

可按照图 3-2 排除此类故障。

华为专有和保密信息
版权所有 © 华为技术有限公司

图 3-2 Eth-Trunk 接口转发不通故障诊断流程图



故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查 Eth-Trunk 接口成员口是否存在故障。

在任意视图下执行命令 **display eth-trunk 1** 查看 Eth-Trunk 接口状态。

```
[Router] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL         Hash arithmetic:According to SA-XOR-DA
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
```


版权所有 © 华为技术有限公司

```
Operate status: down          Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------

PortName          Status      Weight
Ethernet2/0/1     Down        1
Ethernet2/0/2     Down        1
Ethernet2/0/3     Down        1
```

- 如果 Eth-Trunk 接口中成员口的状态为 Down，请执行如下操作：

检查项	检查方法及处理建议
接口是否被人为 **shutdown**	在系统视图下执行 **interface** *interface-type interface-number* 进入故障接口视图，然后执行 **display this** 命令查看接口是否执行了 **shutdown** 操作，如果是请在接口下执行 **undo shutdown** 命令。
链路故障	更换 RouterA 和 RouterB 之间的连接线缆。 **说明** 如果 RouterA 和 RouterB 之间是通过双绞线连接，需要考虑双绞线支持的最大传输距离和实际 RouterA 和 RouterB 之间的距离匹配。
Router 接口故障	将其他空闲接口配置成成员接口。

  执行完上述操作后，接口仍无法 Up，请执行步骤 5。

- 如果成员口的状态是 Up，请同时确保每条线缆两端是否连接到正确的对应设备和对应的接口，完成后如果故障依然存在请执行步骤 2。

步骤 2 检查设备两端的 Eth-Trunk 接口包含的成员口信息。

查看 RouterA 和 RouterB 上 Eth-Trunk 接口包含的成员口信息。

```
[RouterA] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL           Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 1    Max Bandwidth-affected-linknumber: 8
Operate status: up            Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------

PortName          Status      Weight
Ethernet2/0/1      up         1
Ethernet2/0/2      up         1
Ethernet2/0/3      up         1
[RouterB] display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL           Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 4    Max Bandwidth-affected-linknumber: 8
Operate status: up            Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName          Status      Weight
Ethernet2/0/1      up         1
Ethernet2/0/2      up         1
```

- 如果设备两端 Eth-Trunk 接口成员口数不一致，请正确将设备上的物理接口加入 Eth-Trunk 接口。
- 如果设备两端 Eth-Trunk 接口成员口数一致，请执行步骤 3。

步骤 3 查看 Eth-Trunk 接口上是否配置了下限阈值。

分别在 RouterA、RouterB 上执行命令 **display eth-trunk 1** 查看 Eth-Trunk 接口配置信息。

```
[RouterA] display eth-trunk 1
Eth-Trunk1's state information is:
```


版权所有 © 华为技术有限公司

```
WorkingMode: NORMAL          Hash arithmetic: According to SA-XOR-DA
Least Active-linknumber: 4   Max Bandwidth-affected-linknumber: 8
Operate status: down         Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName         Status      Weight
Ethernet2/0/1     up         1
Ethernet2/0/2     up         1
Ethernet2/0/3     up         1
```

从上述显示信息可以看出，Eth-Trunk 接口上配置了下限阈值 4，而 Eth-Trunk 接口中状态为 Up 的成员口数实际上只有 3 个，这导致的 Eth-Trunk 接口状态为 Down。

- 如果 Eth-Trunk 接口上配置了下限阈值，且下限阈值大于 Eth-Trunk 接口中状态为 Up 的成员口，请正确配置下限阈值。
- 如果 Eth-Trunk 接口上没有配置下限阈值，请执行**步骤 4**。

步骤 4 查看 Eth-Trunk 接口是否是静态 LACP 模式。

分别在 RouterA、RouterB 上执行命令 **display eth-trunk 1** 查看 Eth-Trunk 接口配置信息。

```
[RouterA] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                    WorkingMode: STATIC
Preempt Delay: Disabled      Hash arithmetic: According to SA-XOR-DA
System Priority: 32768       System ID: 0018-826f-fc7a
Least Active-linknumber: 1   Max Active-linknumber: 8
Operate status: down         Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName   Status   PortType  PortPri PortNo PortKey PortState Weight
Ethernet2/0/1   Unselect 100M      32768   264    305     11100010  1
Ethernet2/0/2   Unselect 100M      32768   265    305     11100010  1
Ethernet2/0/3   Unselect 100M      32768   266    305     11100011  1
Partner:
--------------------------------------------------------------------------------
ActorPortName   SysPri SystemID        PortPri PortNo  PortKey   PortState
Ethernet2/0/1   0      0000-0000-0000  0       0       0         11100011
Ethernet2/0/2   0      0000-0000-0000  0       0       0         11100011
Ethernet2/0/3   0      0000-0000-0000  0       0       0         11100011
```

- 如果配置了静态 LACP 模式 Eth-Trunk 接口，且成员口没有被选中，说明 LACP 协商不成功。LACP 协商不成功有如下原因：
  - 成员口故障，导致 LACP 协议报文协商超时。

    请尝试将线缆连接到其他空闲端口，同时将接口加入 Eth-Trunk 中。
  - Eth-Trunk 链路两端设备一端配置了静态 LACP 模式 Eth-Trunk，另一端没有配置静态 LACP 模式 Eth-Trunk。

    请正确配置 Eth-Trunk 链路两端设备。

  故障排除后，LACP 成功协商后，Eth-Trunk 接口显示信息如下：

```
[RouterB] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                    WorkingMode: STATIC
Preempt Delay: Disabled      Hash arithmetic: According to SA-XOR-DA
System Priority: 32768       System ID: 0018-826f-fc7a
Least Active-linknumber: 1   Max Active-linknumber: 8
Operate status: up           Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
ActorPortName   Status   PortType  PortPri PortNo PortKey PortState Weight
Ethernet2/0/1   Selected 100M      32768   264    305     11111100  1
Ethernet2/0/2   Selected 100M      32768   265    305     11111100  1
Ethernet2/0/3   Selected 100M      32768   266    305     11111100  1
```


版权所有 © 华为技术有限公司

```
Partner:
--------------------------------------------------------------------------------
ActorPortName    SysPri SystemID        PortPri PortNo  PortKey   PortState
Ethernet2/0/1    32768  0018-823c-c473  32768   2056    305       11111100
Ethernet2/0/2    32768  0018-823c-c473  32768   2057    305       11111100
Ethernet2/0/3    32768  0018-823c-c473  32768   2058    305       11111100
```

如果故障排除后，LACP 仍然无法成功协商，请执行**步骤 5**。

- 如果没有配置静态 LACP 模式 Eth-Trunk 接口，请执行**步骤 5**。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

3.1.2 故障案例

Eth-Trunk 链路两端聚合方式不一致导致设备两端不能互相 ping 通

网络环境

在图 3-3 的网络中，RouterA 为 AR2200-S，RouterB 为其他厂商设备。两设备之间做链路聚合，将两条 Ethernet 链路进行捆绑，两边完成配置以后，发现无法互相 Ping 通对方的管理地址。

图 3-3 Eth-Trunk 链路两端聚合方式不一致导致设备两端不能互相 Ping 通的组网图

故障分析

1. 在 RouterA 上执行 **display current-configuration interface eth-trunk** 命令，检查 RouterA 的 Eth-Trunk 接口所属的 VLAN。发现两端的 Eth-Trunk 接口在同一 VLAN 内。
2. 在 RouterA、RouterB 上检查以太网接口是否为直连接口，发现以太网接口为直连接口。

版权所有 © 华为技术有限公司

3. 在 RouterA 上执行 **display interface** 命令检查以太网接口的状态是否为 Up，发现以太网接口的状态为 Up，同时确认对端以太网接口的状态也为 Up。
4. 在 RouterA 和 RouterB 上执行 **display trunkmembership eth-trunk** 命令检查 Eth-Trunk 的成员接口数目，发现 RouterA 和 RouterB 的 Eth-Trunk 成员接口数目相同。
5. 在 RouterA 上执行 **display mac-address** 命令查看 MAC 地址学习情况，发现 RouterA 已经学习到了对端的 MAC 地址，但在 RouterB 上查看 MAC 地址表，发现 RouterB 并没有学习到 RouterA 的 MAC 地址。此时怀疑可能是对端链路聚合建立出了问题。最后确认发现对端使能了 LACP，因为 Huawei AR2200-S 系列采用手工聚合方式不进行 LACP 协商，所以 RouterB 发送的 LACP 协商请求 RouterA 并未做应答导致链路聚合没有建立成功。

操作步骤

步骤 1 在 RouterB 上关闭 LACP 协商，RouterA 和 RouterB 能够互相 Ping 通，问题解决。

----结束

案例总结

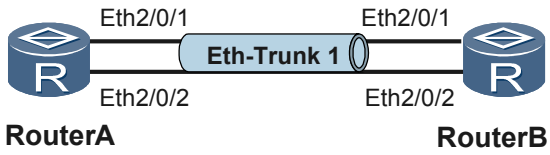
在与其他厂商设备做链路聚合对接时，一定要确保双方采用的聚合方式一致。

Eth-Trunk 两端成员接口数目不一致导致 Eth-Trunk 两端不能互通

网络环境

在图 3-4 的网络中配置 Eth-Trunk。

图 3-4 Eth-Trunk 组网图



配置完成后，发现两台 Router 之间的数据不能正常转发。

故障分析

1. 依次在 RouterA、RouterB 上执行 **display current-configuration interface eth-trunk** 命令，检查两端的 Eth-Trunk 接口是否在同一 VLAN 内。发现两端的 Eth-Trunk 接口在同一 VLAN 内。
2. 依次在 RouterA、RouterB 上检查以太网接口是否为直连接口，发现以太网接口为直连接口。
3. 依次在 RouterA、RouterB 上执行 **display interface** 命令检查以太网接口的状态是否为 Up，发现以太网接口的状态为 Up。
4. 依次在 RouterA、RouterB 上执行 **display trunkmembership eth-trunk** 命令检查两侧 Eth-Trunk 的成员接口数目是否一致，发现 RouterA 的 Eth-Trunk 成员接口数目

版权所有 © 华为技术有限公司

为 2，RouterB 的 Eth-Trunk 成员接口数目为 1（即接口 Eth2/0/1）。两侧 Eth-Trunk 的成员接口数目不一致，造成 Eth-Trunk 之间不能互通。

说明

以下操作均在 RouterA 上执行。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **eth-trunk** *trunk-id*，将接口 Eth/0/2 加入到 Eth-Trunk 1 中。

步骤 4 执行命令 **return** 退回到用户视图，执行命令 **save**，保存对配置的修改。

完成上述操作后，查看数据转发正常，故障排除。

----结束

案例总结

互连的 Eth-Trunk 两端的成员接口数量必须相等，否则会导致数据不能正确转发。

版权所有 © 华为技术有限公司

4 局域网类

关于本章

4.1 VLAN 故障处理

4.2 MAC 表故障处理
介绍 MAC 表常见故障的定位思路。

4.3 MSTP 故障处理

4.4 透明网桥故障处理
介绍了透明网桥常见故障原因及其诊断流程、处理步骤和相关告警与日志。

版权所有 © 华为技术有限公司

4.1 VLAN 故障处理

4.1.1 VLAN 内不能互通的定位思路

介绍了基于端口的 VLAN 内互通故障原因及其诊断流程、处理步骤、相关告警与日志和常用定位命令。

常见原因

基于端口的 VLAN 内端口之间不能互通的常见原因：

- 链路故障。
- 接口被人为 ShutDown 或物理接口损坏。
- 设备 MAC 地址学习错误。
- 设备上配置了端口隔离。
- 主机配置了错误的静态 ARP。
- 设备上配置了错误的端口和 MAC 地址绑定。

说明

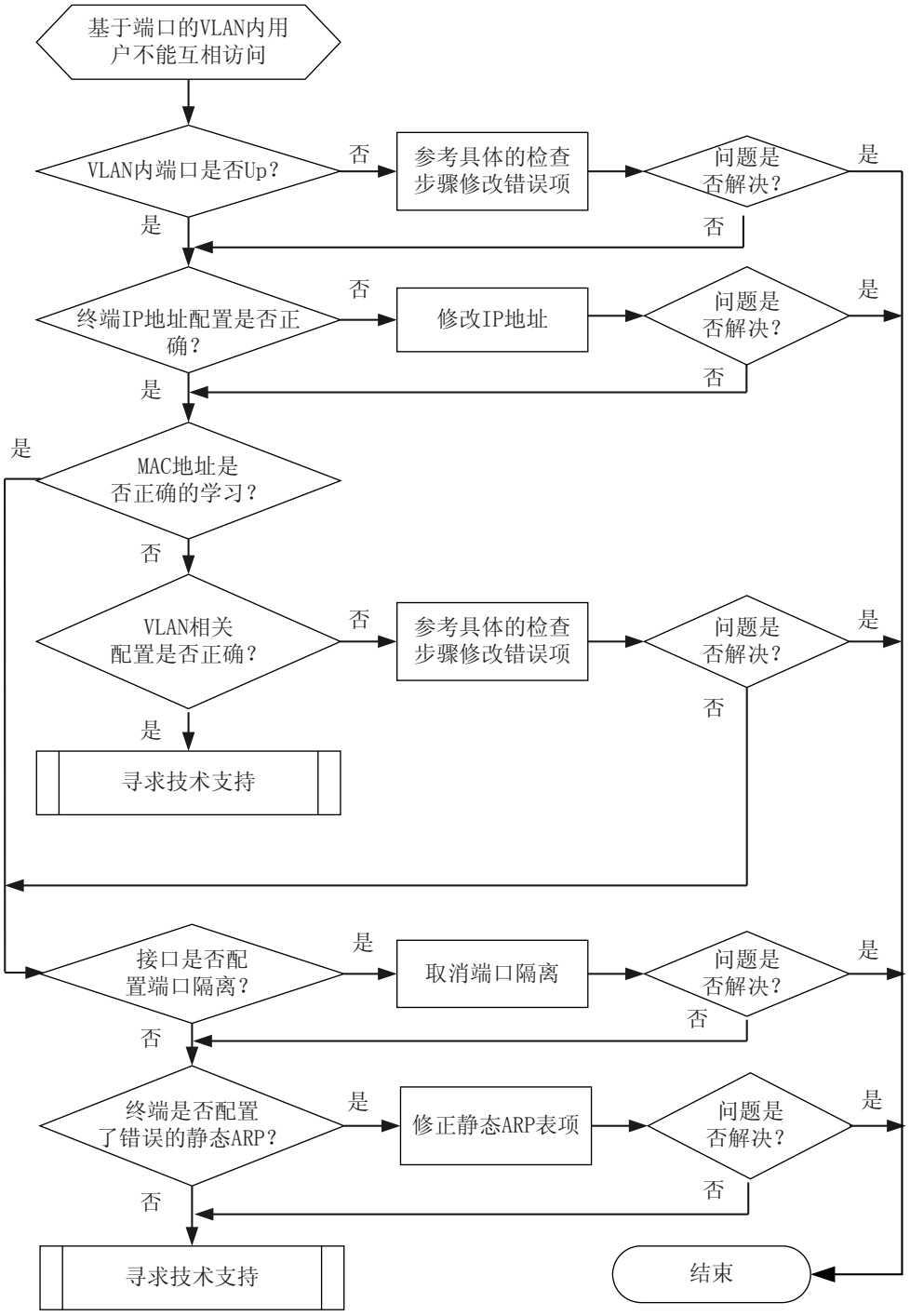
VLAN 间的故障处理请参考 IP 转发类故障处理。

故障诊断流程

可按照图 4-1 排除此类故障。

版权所有 © 华为技术有限公司

图 4-1 基于端口划分的 VLAN 内用户之间不能互通



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查 VLAN 内需要互通的端口是否 Up。

在任意视图下执行 **display interface** *interface-type interface-number* 命令查看需要互通的端口的运行状态。

- 如果接口的状态为 Down，请先执行如下检查：

检查项	检查方法及处理建议
接口是否被人为 **shutdown**	在系统视图下执行 **interface** *interface-type interface-number* 进入故障接口视图，然后执行 **display this** 命令查看接口是否执行了 **shutdown** 操作，如果是请在接口下执行 **undo shutdown** 命令。
链路故障	更换终端与 Router 之间的连接线缆。 **说明** 如果终端与 Router 之间是通过双绞线连接，需要考虑双绞线支持的最大传输距离和实际终端与 Router 之间的距离匹配。
接口双工、速率是否一致	在接口视图下通过执行 **speed**、**duplex** 和 **negotiation auto** 调整终端和 Router 之间速率、双工匹配。
Router 接口故障	尝试将故障接口线缆连接到其他空闲接口。

- 如果成员口的状态是 Up，请执行**步骤 2**。

步骤 2 检查需要互通的终端 IP 地址是否在同一网段，如果不是请修改为同一网段，如果故障仍然存在请执行**步骤 3**。

步骤 3 检查 Router 上 MAC 地址表项是否正确。

在 Router 上执行 **display mac-address** 检查设备学习到 MAC 地址、MAC 地址对应接口、所属 VLAN 是否正确，如果不正确请在接口上执行 **undo mac-address** *mac-address* **vlan** *vlan-id* 命令使 Router 重新学习指定的 MAC 地址。

执行完上述操作后，再检查设备学习到 MAC 地址、MAC 地址对应接口、所属 VLAN 是否正确：

- 如果不正确请执行**步骤 4**。
- 如果正确但用户仍无法互相访问请执行**步骤 5**。

步骤 4 检查 VLAN 相关配置是否正确。

- 请执行如下操作检查 VLAN 相关配置是否正确。

检查项	检查方法及处理建议
需要互通的端口所在的 VLAN 是否已经创建	在任意视图下 执行 **display vlan** *vlan-id* 查看需要互通的端口所在的 VLAN 是否已经创建，如果未创建请在系统视图下执行 **vlan** 命令创建 VLAN。

版权所有 © 华为技术有限公司

检查项	检查方法及处理建议
检查需要互通的接口是否加入VLAN	执行 **display vlan** *vlan-id* 检查需要互通的接口是否已经加入指定 VLAN，如果未加入请将接口加入指定 VLAN。 **说明** 如果需要互通的接口不在同一个设备，还需要考虑设备互联的接口允许指定的 VLAN 通过。 ● Access 类型接口加入 VLAN。根据需要可以选择如下方式将 Access 类型接口加入 VLAN。 **说明** 缺省情况下，Router 的接口类型为 Hybrid。在选择以 Access 方式将接口加入 VLAN 时如果接口类型不是 Access，需要先使用 **port link-type Access** 命令将接口类型修改为 Acess 类型。 1. 在接口视图下执行命令 **port default vlan** 将 Access 类型的接口加入 VLAN。 2. 在 VLAN 视图下执行命令 **port** 将 Access 类型的接口加入 VLAN。 ● Trunk 类型接口加入 VLAN。 **说明** 缺省情况下，Router 的接口类型为 Hybrid。在选择以 Trunk 方式将接口加入 VLAN 时如果接口类型不是 Trunk，需要先使用 **port link-type trunk** 命令将接口类型修改为 Trunk 类型。 在接口视图下执行命令 **port trunk allow-pass vlan** 将 Trunk 类型的接口加入 VLAN。 ● Hybrid 类型接口加入 VLAN。根据需要可以选择如下方式将 Hybrid 类型接口加入 VLAN。 **说明** 缺省情况下，Router 的接口类型为 Hybrid。在选择以 Hybrid 方式将接口加入 VLAN 时如果接口类型不是 Hybrid，需要先使用 **port link-type Hybrid** 命令将接口类型修改为 Hybrid 类型。 1. 在接口视图下执行命令 **port hybrid tagged vlan** 将 Hybrid 类型的接口加入 VLAN。 2. 在接口视图下执行命令 **port hybrid untagged vlan** 将 Hybrid 类型的接口加入 VLAN。
接口和终端是否按照规划的对应关系进行连接	按照正确的对应关系将终端与设备接口进行连接。

执行完上述操作后：

- MAC 地址表项正确，但故障仍然存在，请执行**步骤 5**。
- MAC 地址表项不正确，请执行**步骤 7**。

步骤 5 检查设备上是否配置了端口隔离。

在系统视图下执行 **interface** *interface-type interface-number* 进入故障接口视图，然后执行 **display this** 命令查看接口是否配置了端口隔离：

- 如果未配置端口隔离请执行**步骤 6**。

版权所有 © 华为技术有限公司

- 如果配置了端口隔离，请使用 **undo port-isolate enable** 命令取消端口上端口隔离配置。取消端口隔离后如果故障依然存在请执行**步骤 6**。

步骤 6 检查终端设备上是否配置了错误的静态 ARP 表项，如果终端设备上配置了错误的静态 ARP 表项请修正，完成后如果故障仍然存在请执行**步骤 7**。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

4.2 MAC 表故障处理

介绍 MAC 表常见故障的定位思路。

4.2.1 设备上无法创建正确的 MAC 表项故障处理思路

介绍无法创建正确 MAC 表项的常见原因、诊断流程和详细的处理步骤。

常见原因

本类故障的常见原因主要包括：

- 配置错误导致 MAC 地址学习错误
- 网络中存在环路导致 MAC 地址不断刷新学习
- 设备端口配置了 MAC 地址学习去使能
- 配置了黑洞 MAC 和 MAC 学习限制
- MAC 表项超过设备规格

故障诊断流程

二层数据转发失败，设备上无法创建正确的 MAC 转发表项。

故障的定位思路如下：

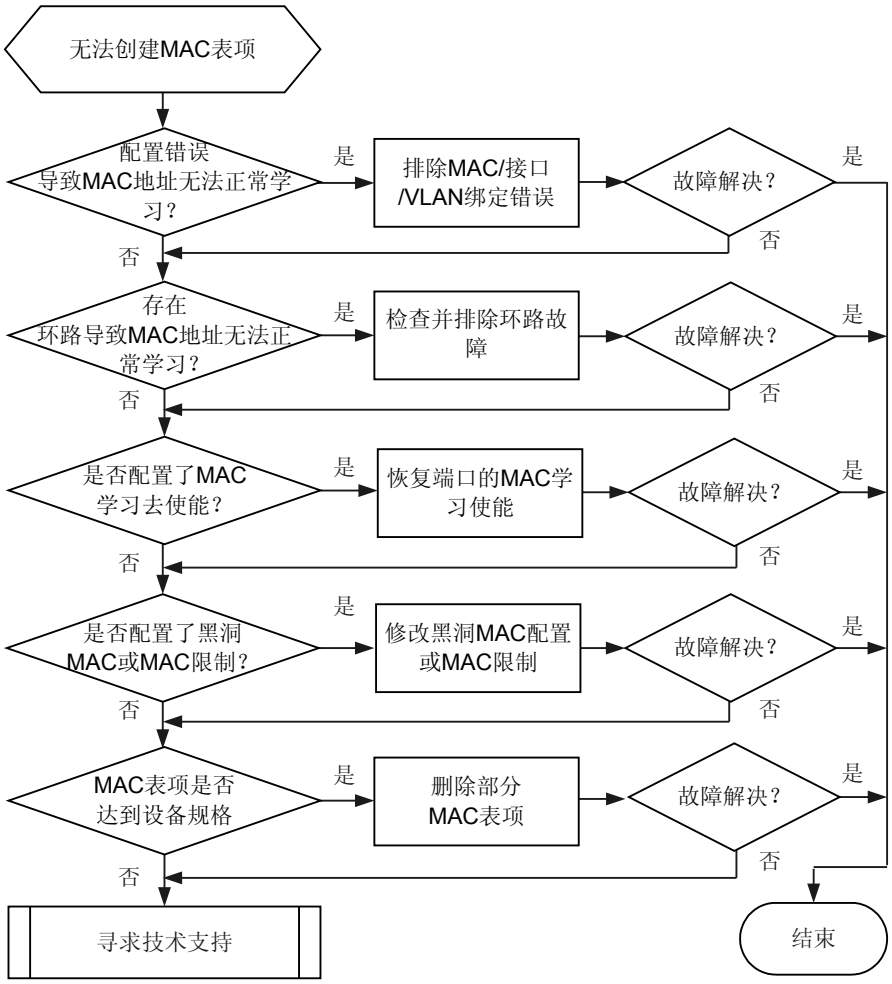
- 检查是否出接口与 VLAN 绑定错误导致接口无法正确学习 MAC 地址
- 检查是否存在环路导致接口学习 MAC 地址错误

版权所有 © 华为技术有限公司

- 检查是否存在其他冲突配置或限制导致接口无法正确学习 MAC 表项
- 检查是否已存在 MAC 表项或超出规格

详细处理流程如图 4-2 所示。

图 4-2 无法创建 MAC 表项 故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 查看是否配置错误导致 MAC 地址无法正确学习。

在系统视图下执行 **display mac-address** 命令，检查 MAC 地址、VLAN 和设备端口的绑定关系是否正确。

```
<Huawei> display mac-address 000f-e207-f2e0
--------------------------------------------------------------------------------
```


版权所有 © 华为技术有限公司

```
MAC Address    VLAN/Bridge                      Learned-From         Type
--------------------------------------------------------------------------------
0025-9e80-2494   1/-                            Eth 2/0/1            dynamic

--------------------------------------------------------------------------------
Total items displayed = 1
```

如果端口/VLAN 配置关系错误，需要重新配置 MAC 地址、VLAN 和设备端口的绑定关系。

如果端口/VLAN 配置无误，请执行**步骤 2**。

步骤 2 检查网络中是否存在环路引起广播风暴，导致 MAC 表项振荡。

如果系统中存在环路，可以采取如下方式来防止 MAC 表振荡：

- 排除环路故障，请参见环路故障处理。
- 在 VLAN 视图下执行命令 **loop-detect eth-loop**，配置 MAC 地址漂移检测功能。配置 MAC 地址漂移检测功能后系统将检测该 VLAN 内所有 MAC 地址是否发生移动，判断是否出现 MAC 地址漂移，若出现 MAC 地址漂移则执行阻断动作。

如果系统中不存在环路，请执行**步骤 3**。

步骤 3 检查是否配置了 MAC 学习去使能。

在接口视图和 VLAN 视图下，查看是否配置了 MAC 地址学习去使能。

```
[Huawei-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
 mac-address learning disable
 port hybrid tagged vlan 10
 undo negotiation auto
#
return
[Huawei-vlan10]display this
 #
vlan 10
 mac-address learning disable
#
return
```

如果显示信息中出现“**mac-address learning disable**”字段表示接口或 VLAN 已经去使能 MAC 地址学习功能。

- 如果接口和 VLAN 去使能 MAC 地址学习功能，请在接口和 VLAN 视图下执行命令 **undo mac-address learning disable** 使能接口学习 MAC 地址功能。
- 如果接口没有去使能 MAC 地址学习功能，请执行**步骤 4**。

步骤 4 检查是否配置了黑洞 MAC 或基于接口的 MAC 地址限制。

在设备上检查是否存在以下配置导致报文在接口被丢弃：

- 是否配置了黑洞 MAC

  执行 **display mac-address blackhole** 命令，查看是否配置了黑洞 MAC。

```
[Huawei] display mac-address blackhole
M--------------------------------------------------------------------------------
MAC Address    VLAN/Bridge                      Learned-From         Type
--------------------------------------------------------------------------------
0001-0001-0001 3333/-                           -                    blackhole

--------------------------------------------------------------------------------
Total items displayed = 1
```

  如果有黑洞 MAC 相关配置，请执行 **undo mac-address blackhole** 命令删除黑洞 MAC 地址。

版权所有 © 华为技术有限公司

- 是否配置了基于接口/VLAN 的 MAC 地址学习限制
  - 在接口/VLAN 视图下执行 **display this** 命令，如存在 **mac-limit maximum** 字段配置，则配置了 MAC 学习限制，此时可以采取如下操作：
    - 请在对应的视图下执行命令 **undo mac-limit** 取消 MAC 地址限制。
    - 请在对应的视图下执行命令 **mac-limit** 调整 MAC 地址学习数量。
  - 在接口视图下执行 **display this** 命令，如存在 **port-security max-mac-num** 或 **port-security enable** 字段配置，则配置了接口配置了安全 MAC 学习限制数量，此时可以采取如下操作：

    说明

    使能接口安全功能后，缺省情况下，接口学习的 MAC 地址限制数量为 1。
    - 在接口视图下执行命令 **undo port-security enable** 取消接口安全功能。
    - 在接口视图下执行命令 **port-security max-mac-num** 修改接口安全 MAC 学习限制数量。

执行完上述操作后，故障仍然存在，请执行**步骤 5**。

步骤 5 检查 MAC 表项是否已达设备支持的最大规格。

在设备上执行 **display mac-address summary** 命令，查看设备目前学习到 MAC 地址数量是否达到产品支持的规格。

- 如果目前设备学习到 MAC 地址数量达到产品支持的规格，则无法继续创建 MAC 表项,此时执行命令 **display mac-address** 查看设备学习的 MAC 地址表。
  - 如果某接口学习到的 MAC 地址远大于接口所连接网络实际运行的主机数，说明该接口所连接的网络可能有恶意刷新 MAC 地址表项的攻击存在，此时：
    - 如果该接口连接其他设备，则在该接口连接的设备上执行命令 **display mac-address** 查看 MAC 地址学习表项，根据 MAC 地址学习接口找到可能存在攻击的主机所在的接口。如果查找到的接口还下连其他设备，请重复上述操作直至查找到恶意攻击的主机。
    - 如果该接口连接一台主机，可以尝试做如下操作：
      - 和管理员确认后先断开该主机，等该主机恶意攻击排除后再接入网络。
      - 和管理员确认后在该接口上执行 **port-security enable** 命令配置接口安全功能或执行 **mac-limit** 命令配置接口 MAC 地址学习数量为 1。
    - 如果该接口连接的是 HUB，可以尝试如下操作：
      - 通过镜像和抓包软件分析该接口收到的报文，根据报文的特征找到攻击主机，找到攻击主机后，和管理员确认后先断开该主机，等该主机恶意攻击排除后再接入网络。
      - 和管理员确认后，分别尝试断开 HUB 连接的主机，通过断开某主机看故障是否存在来判断可能存在攻击的主机，找到攻击主机后，和管理员确认后先断开该主机，等该主机恶意攻击排除后再接入网络。
  - 如果接口学习到的 MAC 地址数量≤该接口连接的实际运行的主机数，说明设备接入的主机已经超过了设备支持的规格，请调整网络部署。
- 如果目前设备学习到 MAC 地址数量未达到产品支持的规格，请执行**步骤 6**。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警与日志

相关告警

无

相关日志

无

4.3 MSTP 故障处理

4.3.1 MSTP 拓扑变化导致业务中断的定位思路

常见原因

配置 MSTP 后，MSTP 拓扑变化导致业务中断。

本类故障的常见原因有：

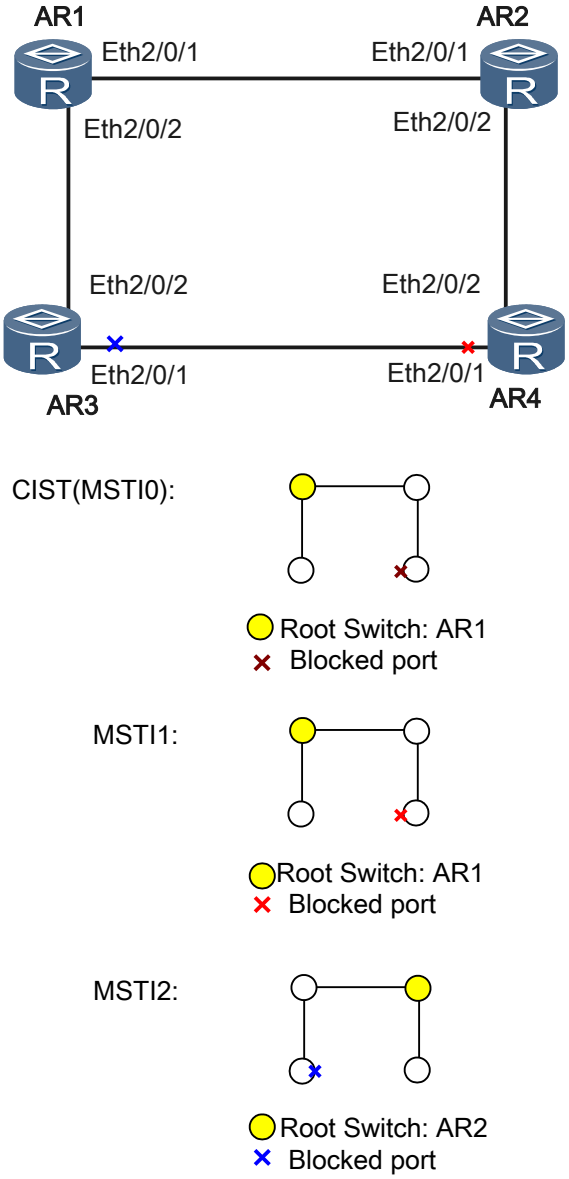
- MSTP 配置错误。
- 物理链路发生震荡，触发设备发送大量 TC 报文。
- 使能 MSTP 的设备收到客户端或透传的 MSTP TC 报文。

故障诊断流程

如图 4-3 所示，MSTP 拓扑变化导致业务中断的故障处理将基于该网络。

版权所有 © 华为技术有限公司

图 4-3 MSTP 功能组网图



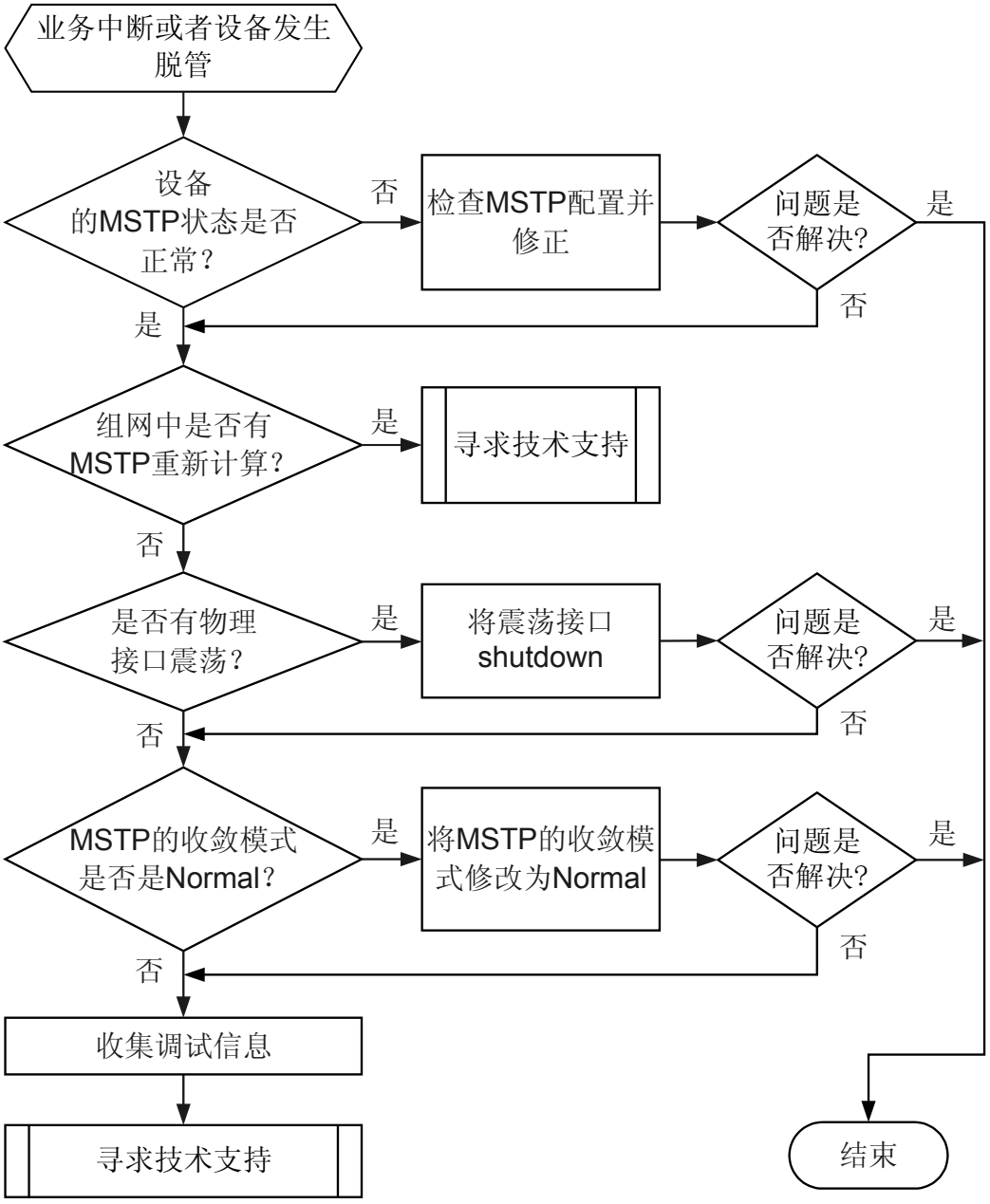
故障诊断思路：

- 检查设备的 MSTP 状态是否正常。
- 检查设备是否收到 TC 报文。
- 检查是否有物理接口震荡。
- 检查 MSTP 的收敛方式是否是 Normal。

可按照图 4-4 排除此类故障。

版权所有 © 华为技术有限公司

图 4-4 MSTP 拓扑变化导致业务中断故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 MSTP 组网内的端口状态是否正常。

查看 MSTP 的端口状态，确认每个端口在每个实例的连通性。

版权所有 © 华为技术有限公司

如图 4-3 所示组网中只有一个 MSTP 环，每个实例应该只有一个阻塞口。通过在每台设备上执行命令 **display stp brief**，可以查看各设备端口状态是否正常。

在任意视图下执行命令 **display stp brief** 查看设备 AR1 的 MSTP 状态信息。如图 4-3 所示，设备 AR1 在实例 0 和实例 1 中都是根桥，所有端口的角色应该都是指定端口。在实例 2 中，设备 AR1 的一个端口为指定端口另一个端口是根端口。转发状态应该是 FORWARDING。

```
[AR1] display stp brief
 MSTID      Port           Role  STP State       Protection
   0        Ethernet2/0/1  DESI  FORWARDING      NONE
   0        Ethernet2/0/2  DESI  FORWARDING      NONE
   1        Ethernet2/0/1  DESI  FORWARDING      NONE
   1        Ethernet2/0/2  DESI  FORWARDING      NONE
   2        Ethernet2/0/1  ROOT  FORWARDING      NONE
   2        Ethernet2/0/2  DESI  FORWARDING      NONE
```

在任意视图下执行命令 **display stp brief** 查看设备 AR2 的 MSTP 状态信息。如图 4-3 所示，设备 AR2 在实例 2 中是根桥，所有端口角色应该都是指定端口。设备 AR2 在其他实例的端口角色为指定端口和根端口。转发状态应该都是 FORWARDING。

```
[AR2] display stp brief
 MSTID      Port           Role  STP State       Protection
   0        Ethernet2/0/1  ROOT  FORWARDING      NONE
   0        Ethernet2/0/2  DESI  FORWARDING      NONE
   1        Ethernet2/0/1  ROOT  FORWARDING      NONE
   1        Ethernet2/0/2  DESI  FORWARDING      NONE
   2        Ethernet2/0/1  DESI  FORWARDING      NONE
   2        Ethernet2/0/2  DESI  FORWARDING      NONE
```

在任意视图下执行命令 **display stp brief** 查看设备 AR3 的 MSTP 状态信息。如图 4-3 所示，实例 2 的阻塞端口在本设备上，端口角色分别是根端口和 Alternate 端口，其中 Alternate 端口转发状态是 DISCARDING。在其他实例中，设备 AR3 的端口角色分别是指定端口和根端口，转发状态是 FORWARDING。

```
[AR3] display stp brief
 MSTID      Port           Role  STP State       Protection
   0        Ethernet2/0/1  DEST  FORWARDING      NONE
   0        Ethernet2/0/2  ROOT  FORWARDING      NONE
   1        Ethernet2/0/1  DEST  FORWARDING      NONE
   1        Ethernet2/0/2  ROOT  FORWARDING      NONE
   2        Ethernet2/0/1  ALTE  DISCARDING      NONE
   2        Ethernet2/0/2  ROOT  FORWARDING      NONE
```

在任意视图下执行命令 **display stp brief** 查看设备 AR4 的 MSTP 状态信息。如图 4-3 所示，实例 0 和实例 1 的阻塞端口在本设备上，端口角色分别是根端口和 Alternate 端口，其中 Alternate 端口转发状态是 DISCARDING。在实例 2 中，设备 AR4 的端口角色分别是指定端口和根端口，转发状态是 FORWARDING。

```
[AR4] display stp brief
 MSTID      Port           Role  STP State       Protection
   0        Ethernet2/0/1  ALTE  DISCARDING      NONE
   0        Ethernet2/0/2  ROOT  FORWARDING      NONE
   1        Ethernet2/0/1  ALTE  DISCARDING      NONE
   1        Ethernet2/0/2  ROOT  FORWARDING      NONE
   2        Ethernet2/0/1  DESI  FORWARDING      NONE
   2        Ethernet2/0/2  ROOT  FORWARDING      NONE
```

- 对于如图 4-3 所示组网，每个实例有且只有一个阻塞状态（DISCARDING）的端口，其他端口的状态均是转发状态（FORWARDING）。如果出现多个阻塞端口，说明 MSTP 计算问题，请执行步骤 6。
- 如果 MSTP 状态正确，请执行步骤 2。

步骤 2 检查 MSTP 配置是否正确。

版权所有 © 华为技术有限公司

执行命令 **display stp region-configuration** 检查 VLAN 与实例之间的映射关系。

```
[AR1] display stp region-configuration
Oper Configuration:
   Format selector :0
   Region name     :huawei
   Revision level  :0

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

- 查看 VLAN 与实例之间的映射关系是否正确。若出现映射关系错误，请执行命令 **instance** 将指定 VLAN 映射到指定的生成树实例上，并执行命令 **active region-configuration** 激活 **instance** 命令配置的 VLAN 与实例之间的映射关系。

执行命令 **display current-configuration** 获取设备的配置文件，查看设备上 MSTP 的相关配置。

- 与用户终端设备相连的端口 MSTP 是否是处于去使能状态或配置为边缘端口。
- 查看设备端口是否加入正确的 VLAN。正确的 VLAN 配置请参见《AR2200-S 配置指南-局域网》的 VLAN 配置一节。
- 如果 MSTP 配置正确，请执行**步骤 3**。

步骤 3 查看组网中是否有 MSTP 重新计算。

在任意视图下执行命令 **display stp** 查看设备是否收到 TC 报文。

```
[AR1] display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge          :57344.00e0-fc00-1597
Bridge Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0     .0018-826f-fc7a / 20000
CIST RegRoot/IRPC    :57344.00e0-fc00-1597 / 0
CIST RootPortId      :128.2
BPDU-Protection      :disabled
TC or TCN received   :0
TC count per hello   :0
STP Converge Mode    :Nomal
Time since last TC :2 days 14h:16m:15s

-------[MSTI 1 Global Info]-------
MSTI Bridge ID       :4096.00e0-fc00-1597
MSTI RegRoot/IRPC    :4096.00e0-fc00-1597 / 0
MSTI RootPortId      :0.0
Master Bridge        :57344.00e0-fc00-1597
Cost to Master       :0
TC received          :0
TC count per hello   :2
```

- 如果上述显示信息中 TC or TCN received、TC count per hello、TC received、TC count per hello 中的数值增长，说明设备收到 TC 报文，网络拓扑发生变化。请查看日志 MSTP/6/SET_PORT_DISCARDING 和 MSTP/6/SET_PORT_FORWARDING，通过日志查看使能 MSTP 的端口角色是否有变化。
  - 如果端口角色没有变化，请执行**步骤 4**。
  - 如果端口角色有变化，请执行**步骤 6**。
- 如果上述显示信息中 TC or TCN received、TC count per hello、TC received、TC count per hello 中的数值是 0，说明设备没有收到 TC 报文，请联系华为技术支持工程师。

步骤 4 查看是否有端口震荡。

查看日志 IFNET/4/IF_STATE，通过日志查看使能 MSTP 的端口是否存在 Up 和 Down 状态频繁切换。

版权所有 © 华为技术有限公司

- 如果使能 MSTP 的端口状态在 Up 与 Down 之间不停的变动，则说明端口存在震荡。物理端口频繁的 Up/Down 将导致组网内设备的 MSTP 状态不稳定，并产生大量的 TC 报文，频繁删除 ARP 和 MAC 地址表项，导致业务中断。**shutdown** 震荡的物理端口。如果将震荡端口 **shutdown** 后，业务仍然中断，请执行步骤 5。
- 如果没有震荡端口，请执行步骤 5。

步骤 5 检查 MSTP 的收敛模式是否是 Normal。

在任意视图下执行命令 **display stp** 查看设备 MSTP 收敛模式。

```
[AR1] display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :57344.00e0-fc00-1597
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0    .0018-826f-fc7a / 20000
CIST RegRoot/IRPC   :57344.00e0-fc00-1597 / 0
CIST RootPortId     :128.2
BPDU-Protection     :disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC :2 days 14h:16m:15s

-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :4096.00e0-fc00-1597
MSTI RegRoot/IRPC   :4096.00e0-fc00-1597 / 0
MSTI RootPortId     :0.0
Master Bridge       :57344.00e0-fc00-1597
Cost to Master      :0
TC received         :0
TC count per hello  :2
```

- 如果是 Normal 模式，请执行步骤 6。
- 如果是 Fast 模式，请执行命令 **stp converge normal** 将收敛模式修改为 Normal 模式。如果修改后，业务仍然中断，请执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.1 hwMstpiPortStateForwarding

MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.2 hwMstpiPortStateDiscarding

MSTP_1.3.6.1.2.1.17.0.2 topologyChange

相关日志

MSTP/6/RECEIVE_MSTITC

VOSCPU/4/CPU_USAGE_HIGH

版权所有 © 华为技术有限公司

4.4 透明网桥故障处理

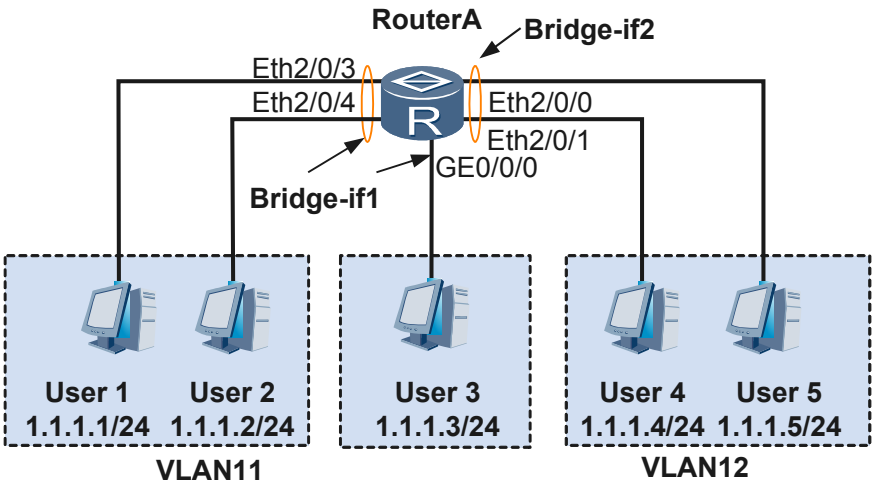
介绍了透明网桥常见故障原因及其诊断流程、处理步骤和相关告警与日志。

4.4.1 桥组内二层转发不通的定位思路

介绍桥组内二层转发不通的故障原因、处理流程和详细的故障处理步骤。

常见原因

图 4-5 桥组内二层转发组网图



如图 4-5 所示，User1 ～ User5 位于同一网段但属于不同的 VLAN，为了实现 VLAN11 中的用户可以和 User3 相互通信，与 VLAN12 中的用户相互隔离，采用了透明网桥的本地桥接功能，将有通信需求的用户加入同一个桥组，没有通信需求的用户加入不同的桥组。不同桥组可以相互隔离，但是同一桥组却无法正常通信，此类故障常见原因有：

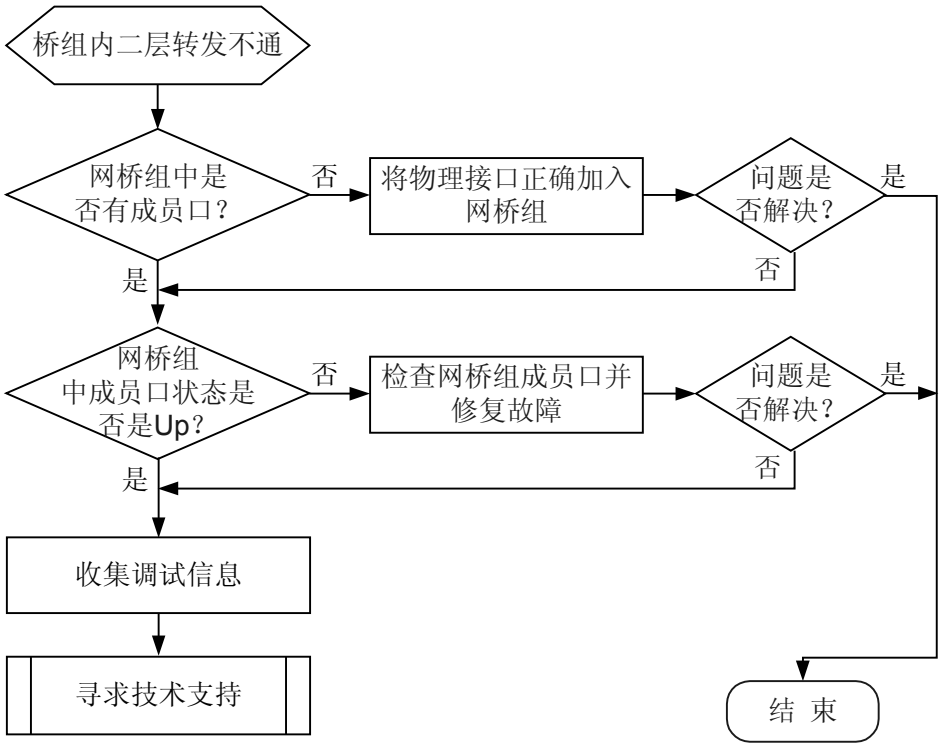
- 物理口加入网桥组失败。
- 网桥组成员口故障。

故障诊断流程

可按照图 4-6 排除此类故障。

版权所有 © 华为技术有限公司

图 4-6 桥组内二层转发不通故障诊断流程图



故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查网桥组中是否有成员口。

在 RouterA 上执行命令 **display bridge information**，查看网桥组中是否有成员口。

```
<RouterA> display bridge information
Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    GigabitEthernet0/0/0 : Up
    Vlanif11 : Up
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    Vlanif12 : Up
```

- 如果网桥组中没有成员口，请将接口正确加入网桥组。

版权所有 © 华为技术有限公司

将接口加入网桥组，请参见《AR2200-S 配置指南-局域网》中的透明网桥配置章节。

- 如果网桥组中已经有成员口，请执行**步骤 2**。

步骤 2 检查网桥组成员口状态是否是 Up。

在 RouterA 上执行命令 **display bridge information**，查看网桥组中成员口的状态。

```
<RouterA> display bridge information
Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    GigabitEthernet0/0/0 : Up
    Vlanif11 : Up
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    Vlanif12 : Up
```

- 如果网桥组成员口状态是 Down，请检查网桥组成员口，如端口是否 Up、协议配置是否正确。
- 如果网桥组成员口状态是 Up，请执行**步骤 3**。

步骤 3 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

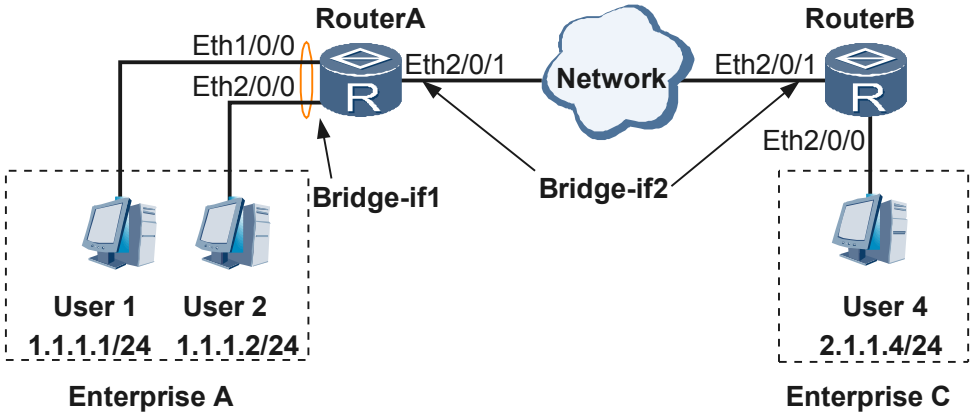
4.4.2 集成路由桥接转发不通的定位思路

介绍集成路由桥接转发不通的故障原因、处理流程和详细的故障处理步骤。

版权所有 © 华为技术有限公司

常见原因

图 4-7 集成路由桥接组网图



如图 4-7 所示，企业 A 和企业 C 位于不同的网段，为了实现不同企业间的通信，采用了透明网桥的集成路由功能。但是不同企业间仍然无法正常通信，此类故障常见原因有：

- 物理口加入网桥组失败。
- 网桥组成员口故障。
- 不同网段用户之间路由不可达。

故障诊断流程

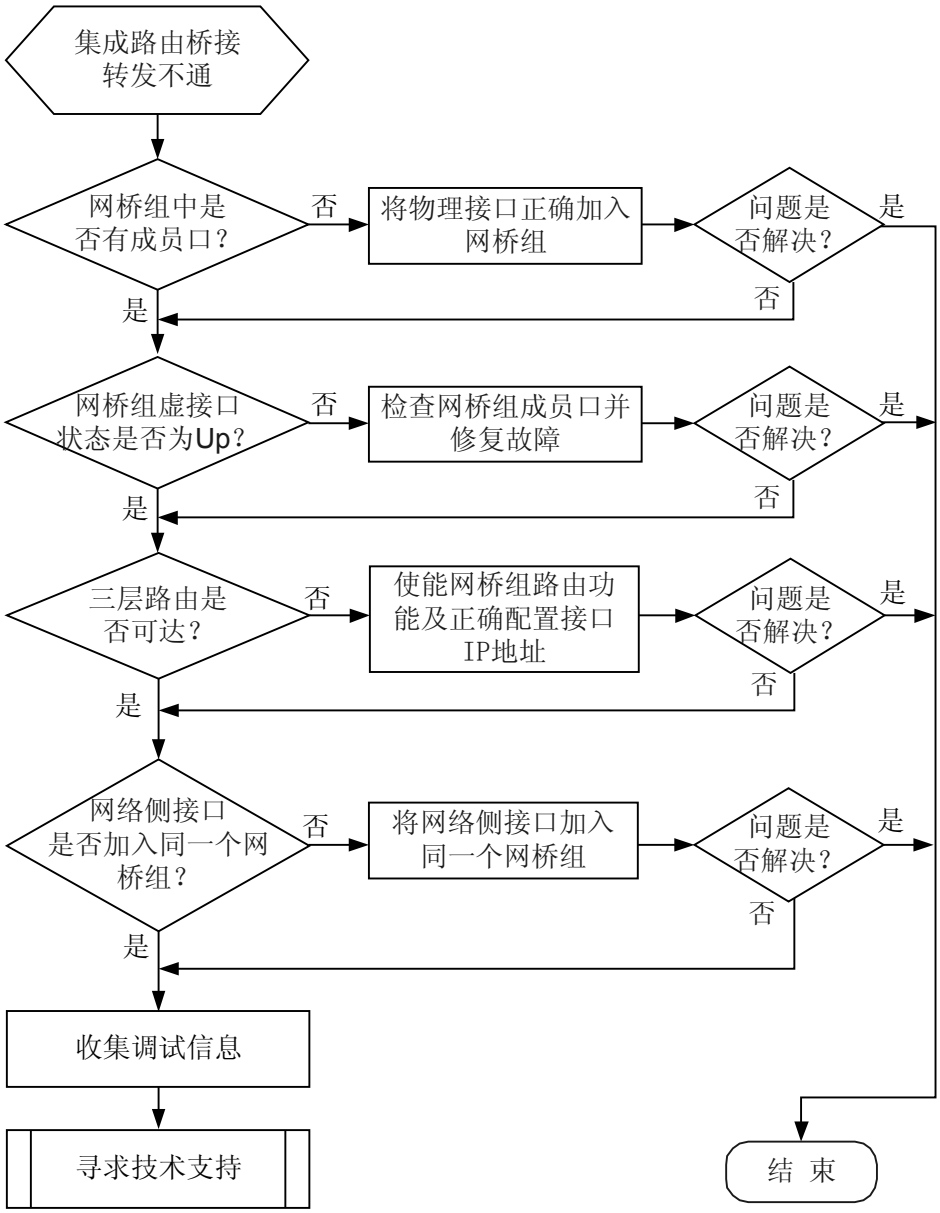
故障诊断思路：

- 检查网桥组中是否有成员口。
- 检查网桥组虚接口状态。
- 检查网桥组成员口是否出现故障。
- 检查网桥组是否使能路由功能，及 IP 地址配置是否正确。
- 收集调试信息。

可按照图 4-8 排除此类故障。

版权所有 © 华为技术有限公司

图 4-8 集成路由桥接转发不通故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查网桥组中是否有成员口。

在 RouterA 上执行命令 **display bridge information**，查看网桥组中是否有成员口。

```
<RouterA> display bridge information
Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
```


版权所有 © 华为技术有限公司

```
    Routing      : IP
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    Ethernet1/0/0 : Up
    Ethernet2/0/0 : Up
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : IP
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    Ethernet2/0/1 : Up
```

- 如果网桥组中没有成员口，请按图 4-7 组网图将物理接口正确加入网桥组。

  将物理接口加入网桥组，请参见《AR2200-S 配置指南-局域网》中的透明网桥配置章节。
- 如果网桥组中已经有成员口，请执行步骤 2。

步骤 2 检查网桥组虚接口状态是否为 Up。

在 RouterA 上执行命令 **display interface bridge-if**，查看网桥组虚接口状态信息。

```
<RouterA> display interface bridge-if
Bridge-if1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-01-07 15:13:49 UTC-08:00
Description:HUAWEI, AR Series, Bridge-if1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.3/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-057a-a000
Physical is BRIDGE-IF
Current system time: 2011-01-07 15:27:12-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 24 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 24 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 11 packets,0 bytes,
           10 unicast,1 broadcast,0 multicast
           0 errors,0 drops,0 unknownprotocol
    Output:13 packets,0 bytes,
           11 unicast,2 broadcast,0 multicast
           0 errors,0 drops
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
Bridge-if2 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-01-07 15:25:34 UTC-08:00
Description:HUAWEI, AR Series, Bridge-if2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 2.2.2.3/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-057a-a000
Physical is BRIDGE-IF
Current system time: 2011-01-07 15:27:12-08:00
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 139 packets,0 bytes,
           0 unicast,0 broadcast,0 multicast
           0 errors,0 drops,0 unknownprotocol
    Output:140 packets,0 bytes,
           0 unicast,0 broadcast,0 multicast
           0 errors,0 drops
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

- 如果网桥组虚接口状态为 Down，请检查网桥组成员口，如端口是否 Up、协议配置是否正确。

版权所有 © 华为技术有限公司

- 如果网桥组虚接口状态是 Up，请执行**步骤 3**。

步骤 3 检查不同网桥组之间路由是否可达。

在 RouterA 上执行命令 Ping，检查不同网桥组之间是否可以 Ping 通。

- 如果不同网桥组之间 Ping 不通，请执行**步骤 4**。
- 如果不同网桥组之间可以 Ping 通，请执行**步骤 5**。

步骤 4 查看网桥组是否使能路由功能。

在 RouterA 上执行命令 **display bridge information**，查看系统当前配置的网桥信息。

```
<RouterA> display bridge information
Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : IP
    MAC learning : Enable
  interface :total 2 interface(s) in the bridge
    Ethernet1/0/0 : Up
    Ethernet2/0/0 : Up
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : IP
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    Ethernet2/0/1 : Up
```

- 如果网桥组未使能路由功能，请在网桥组视图下执行命令 **routing ip** 使能网桥组路由功能。
- 如果网桥组已经使能路由功能，检查网桥组虚拟接口的 IP 地址配置是否正确，及参考《AR2200-S 故障处理》中 IP 转发故障处理章节中的 Ping 不通问题的定位思路。

以上步骤执行完毕后，如果不同网桥组之间仍然 Ping 不通，请执行**步骤 5**。

步骤 5 查看网桥组网络侧的接口是否加入同一个网桥组。

分别在 RouterA、RouterB 上执行命令 **display this**，查看网桥组网络侧接口的配置信息。

查看 RouterA。

```
<RouterA> system-view
[RouterA] interface ethernet2/0/1
[RouterA-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
 bridge 2
 undo shutdown
#
return
```

查看 RouterB。

```
<RouterB> system-view
[RouterB] interface ethernet2/0/1
[RouterB-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
 bridge 2
 undo shutdown
#
return
```


版权所有 © 华为技术有限公司

- 如果网桥组网络侧接口加入的是同一个网桥组，请执行**步骤 6**。
- 如果网桥组网络侧接口没有加入同一个网桥组，请参见《AR2200-S 配置指南-局域网》中的透明网桥配置章节。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

5 广域网类

关于本章

5.1 E1/T1 故障处理

5.2 FR 故障处理

5.3 MFR 故障处理

5.4 DCC 故障处理

5.5 ISDN 故障处理

5.6 PPPoE 故障处理

5.7 PPP 故障处理

5.8 xDSL 故障处理
介绍了 xDSL 常见故障的定位思路和案例。

5.9 3G 故障处理

版权所有 © 华为技术有限公司

5.1 E1/T1 故障处理

5.1.1 E1/T1 接口物理状态正常但数据收发异常的定位思路

常见原因

本类故障的常见原因主要包括：

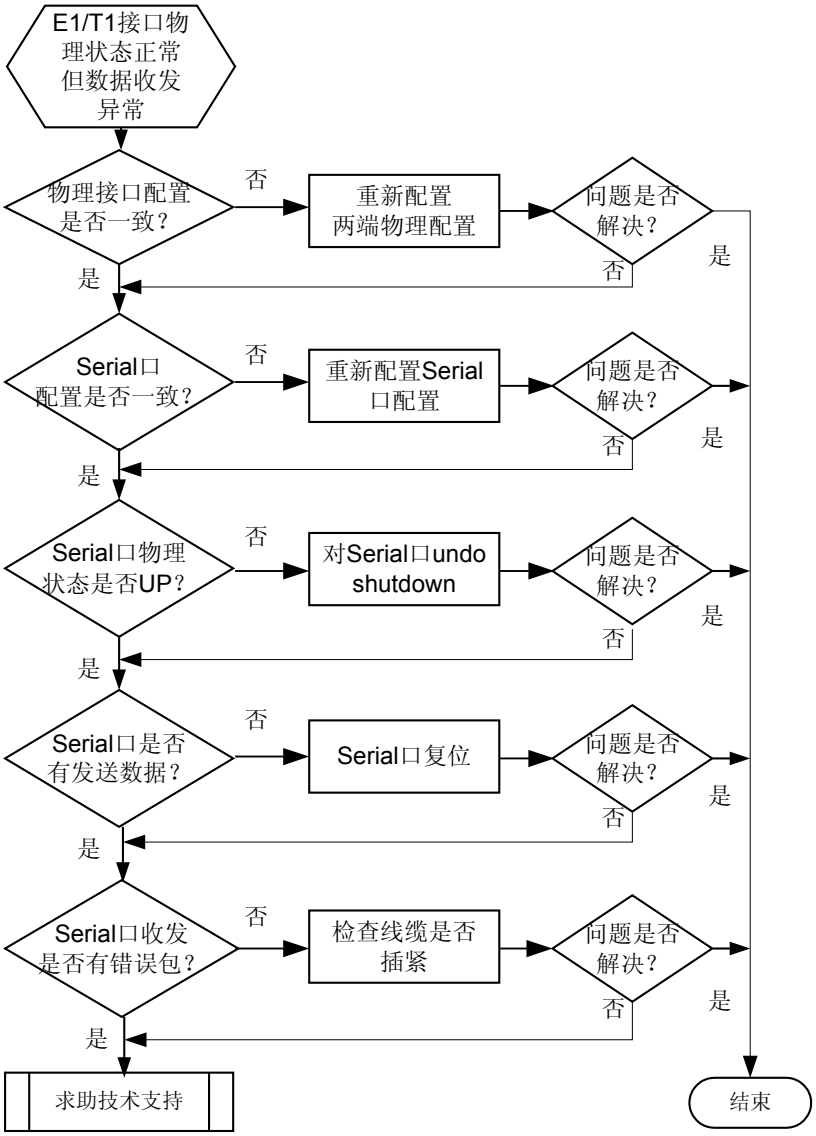
- E1/T1 板上的 CPLD 逻辑版本不正确
- 对接端口的时隙绑定不正确

故障诊断流程

详细故障处理流程，如图 5-1 所示。

版权所有 © 华为技术有限公司

图 5-1 E1/T1 接口物理状态正常但数据收发异常故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查对接物理接口的配置是否一致。

进入 CE1/PRI 接口视图执行 **display this** 命令，查看 CE1/PRI 口配置信息。

```
[Huawei]controller e1 1/0/0
[Huawei-E1 1/0/0]display this
[V200R001C00B000]
#
controller E1 1/0/0
 channel-set 0 timeslot-list 1
frame-format crc4
clock master
```


版权所有 © 华为技术有限公司

```
#
return
```

对比两端接口的物理属性是否一致，比如两端的帧格式是否同为 CRC4 复帧、编码格式是否都是 HDB3、数据是否均为非翻转、同一通道中绑定的时隙号是否一致等，注意时钟需要两端配置成一主一备方式，而不能是同为主或同为备。

- 如果两端配置不一致，或者端口 UP/Down 反复，请对两端重新配置。
- 如果两端配置一致，符合上述要求，并且物理状态始终稳定在 UP，请执行步骤 2。

步骤 2 检查 Serial 口的配置是否一致。

进入 Serial 接口视图执行 **display this** 命令，查看 Serial 口配置信息。

```
[Huawei-E1 1/0/0]int serial 1/0/0:0
[Huawei-Serial1/0/0:0]display this
[V200R001C00B000]
#
interface Serial1/0/0:0
 link-protocol ppp
 timer hold 0
 ip address 1.1.1.2 255.255.255.0
#
return
```

检查对接两端相应的 Serial 口协议配置及物理属性配置是否一致，比如两端都封装了 PPP 协议、都使用默认的 CRC16 等，同时需要查看 Serial 口是否被 Shutdown。

说明

如果两端的 CRC 配置不一致，会因为 CRC 检验出错导致无法正常互通。

- 如果两端的 Serial 口的配置不一致，请重新配置。
- 如果两端的 Serial 口配置是一致的，但数据仍不能正常收发，请执行步骤 3。

步骤 3 检查 Serial 口是否有数据收发。

进入 Serial 口视图执行 **display this interface** 命令，查看 Serial 口的状态。

```
[Huawei-Serial1/0/0:0] display this interface
Serial1/0/0:0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2008-01-08 02:59:55 UTC-05:13
Description:HUAWEI, AR Series, Serial1/0/0:0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Derived from E1 1/0/0,  Timeslot(s) Used: 1,  baudrate is 64000 bps
Internet Address is 1.1.1.2/24
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time   : 2008-01-08 02:59:52 UTC-05:13
Last physical down time : 2008-01-07 22:40:43 UTC-05:13
Current system time: 2008-01-08 03:33:42-05:13
Last 300 seconds input rate 213795 bytes/sec 1710360 bits/sec 4276 packets/sec
Last 300 seconds output rate 213796 bytes/sec 1710368 bits/sec 4276 packets/sec
Input: 140727 packets, 12665430 bytes
  length errors:          0,  giants:                0
  CRC:                    0,  align errors:          0
  aborts:                 0,  no buffers:            0
Output: 0 packets, 0 bytes
  too long errors:        0

    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

- 检查对接两端相应的 Serial 口是否都有发送数据，如果没有发送数据，则说明上层的协商报文没有正常发出，请尝试 Shutdown 和 Undoshutdown 接口触发上层发送报文。

版权所有 © 华为技术有限公司

- 如果存在数据收发，则执行步骤 4。

步骤 4 查看 Serial 口收发是否有错误包。

进入 Serial 口视图执行 **display this interface** 命令，查看 Serial 口的状态。

```
[Huawei-Serial1/0/0:0] display this interface
Serial1/0/0:0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-03-24 13:52:40
Description:HUAWEI, AR Series, Serial1/0/0:0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Derived from E1 4/0/0,  Timeslot(s) Used: 1-31,  baudrate is 1984000 bps
Internet Address is 192.168.22.2/24
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time   : 2011-03-24 13:46:02
Last physical down time : 2011-03-24 13:46:02
Current system time: 2011-03-24 14:03:31
Last 300 seconds input rate 213795 bytes/sec 1710360 bits/sec 4276 packets/sec
Last 300 seconds output rate 213796 bytes/sec 1710368 bits/sec 4276 packets/sec

Input: 2779788 packets, 138980787 bytes
  length errors:           0,  giants:                0
  CRC:                     1,  align errors:          0
  aborts:                  0,  no buffers:            1
Output: 2780617 packets, 139022246 bytes
  too long errors:         0

    Input bandwidth utilization  : 86.21%
    Output bandwidth utilization : 86.21%
```

- 检查对接两端相应的 Serial 口接收数据中是否有大量 CRC 错误包，如果有则检查线缆是否插紧。
- 如果未收到 CRC 错误包，或者收到 CRC 错误包但重新插拔后仍无改善，则执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- CE1/PRI 口 Up 告警：Nov 28 2007 21:13:47+08:00 AR2220 %%01IFPDT/4/IF_STATE (l)[4]:Interface E1 1/0/0 has turned into UP state.
- CE1/PRI 口 Down 告警：Nov 28 2007 21:13:41+08:00 AR2220 %%01IFPDT/4/ IF_STATE(l)[0]:Interface E1 1/0/0 has turned into DOWN state
- Serial 口 Up 告警：May 11 2011 17:21:30 AR2220 %%01IFNET/4/LINK_STATE（l）[3332]:The line protocol PPP IPCP on the interface Serial1/0/0:0 has entered the UP state.
- Serial 口 Down 告警：May 11 2011 17:21:26 AR2220 %%01IFNET/4/LINK_STATE（l）[3330]:The line protocol PPP IPCP on the interface Serial1/0/0:0 has entered the DOWN state.

相关日志

无

版权所有 © 华为技术有限公司

5.2 FR 故障处理

5.2.1 FR 链路协议 UP，但无法 ping 通对端的定位思路

常见原因

可能发生 PING 不通故障的场景包括：

- 基本 FR
- PVC-Group

本类故障的常见原因包括：

- 基本 FR 场景
  1. 接口下未配置 IP 地址
  2. 未生成 Map（PVC 和对端 IP 地址之间的映射）
  3. 生成 Map，但未生成路由
- PVC 组场景
  1. PVC 组中优先级没有分配
  2. PVC 组中没有配置缺省 PVC，且优先级没有完全分配

说明

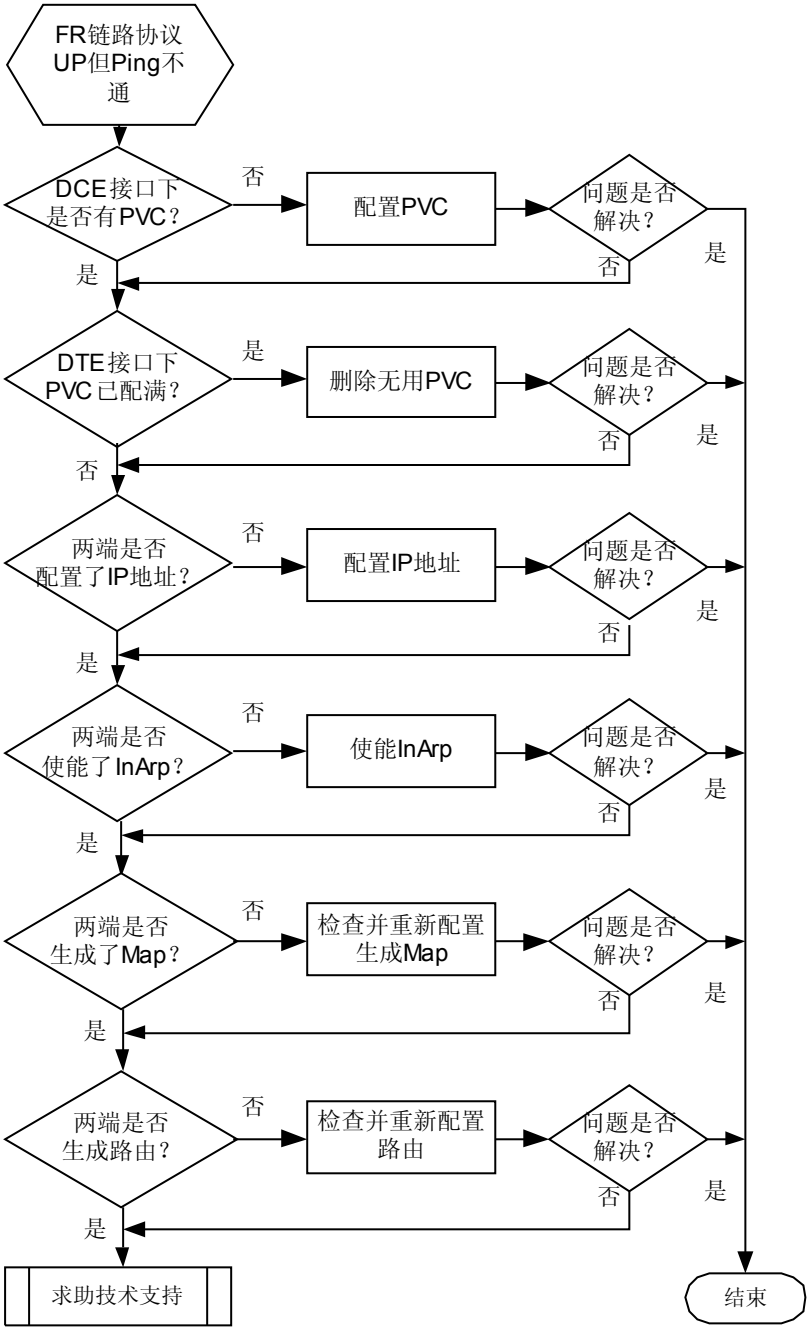
对于转发 PING，除上述各项常见原因外，还需要检查两端是否配置了静态路由。

故障诊断流程

基本 FR 场景详细故障处理流程，如图 5-2 所示。

版权所有 © 华为技术有限公司

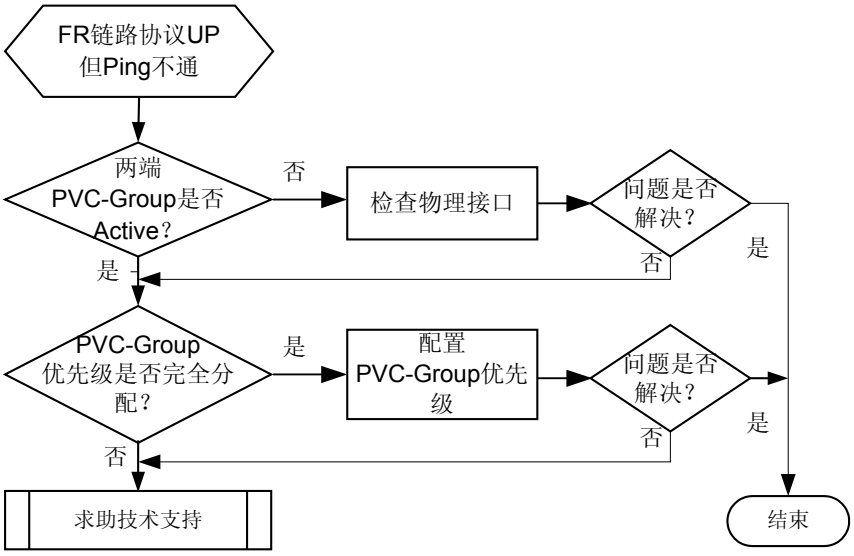
图 5-2 FR 链路协议 UP 但 PING 不通故障诊断流程图



PVC-Group 场景详细故障处理流程，如图 5-3 所示。

版权所有 © 华为技术有限公司

图 5-3 FR 链路协议 UP 但 PING 不通故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

- 基本 FR 场景诊断步骤
  1. 检查 DTE 侧接口下是否有 PVC

     在系统视图下执行 **display fr pvc-info interface Serial** 命令，查看 PVC 状态。

     ```
     [Huawei]display fr pvc-info interface Serial 2/0/0:2
     PVC statistics for interface Serial2/0/0:2 (DTE, physical UP)
         DLCI = 300, USAGE = UNUSED (00000000), Serial2/0/0:2
         create time = 2008/01/03 19:05:54, status = ACTIVE
         InARP = Enable, PVC-GROUP = NONE
         in packets = 0, in bytes = 0
     out packets = 0, out bytes = 0
     ```

     - 如果显示信息中无 PVC 信息，则说明该接口下没有 PVC，请重新在 DCE 侧进行 PVC 配置，或者在 DTE 侧进行 PVC 配置，且确保 DCE 侧配置了 PVC。
     - 如果显示信息中 **status** 字段值为 **INACTIVE**，可能 DCE 侧没有配置 PVC，请重新在 DCE 侧进行 PVC 配置。
     - 如果显示信息中 **status** 字段值为 **ACTIVE**，则说明 PVC 正常，请进行步骤 2。

     说明

     若 DTE 侧使用的是子接口，需要手动在子接口上配置 DLCI。

  2. 查看 DTE 侧的 PVC 是否已经配满

     执行 **display fr pvc-info** 命令，查看当前已有的 PVC。

     ```
     [Huawei]display fr pvc-
     info
     ```


版权所有 © 华为技术有限公司

```
PVC statistics for interface Serial2/0/0:2 (DTE, physical UP)
    DLCI = 300, USAGE = UNUSED (00000000), Serial2/0/0:2
    create time = 2008/01/03 19:05:54, status = ACTIVE
    InARP = Enable, PVC-GROUP = NONE
    in packets = 0, in bytes = 0
    out packets = 0, out bytes = 0
```

如果显示信息中，现有的 PVC 个数已经达到产品的规格限制，就不能再创建 PVC 了。AR2200-S 的 PVC 规格上限为 512。

- 如果因为 PVC 超过规格无法创建，导致 PING 不通，则需要将无用的 PVC 删除。
- 如果 PVC 未超过规格，则进行步骤 3。

说明

只有在 DCE 和 DTE 侧都删除 dlci 才是有效的。

3. 检查两端设备的接口下是否都配置了 IP 地址

   在 FR 接口视图下执行 **display this** 命令，查看此接口下是否配置了 IP 地址。

```
[Huawei-Serial2/0/0:2]display this
[V200R001C00B110]
#
interface Serial2/0/0:2
 link-protocol fr
 ip address 7.7.7.2 255.255.255.0
#
return
```

   - 如果接口下未配置 IP 地址，则在接口下进行配置。
   - 如果接口下已经配置了 IP 地址，则进行步骤 4。

4. 检查接口下是否使能了 InARP

   执行 **display this** 命令，查看当前接口下的配置。

```
[Huawei-Serial2/0/0:2]display this
[V200R001C00B110]
#
interface Serial2/0/0:2
 link-protocol fr
 undo fr inarp
 ip address 7.7.7.2 255.255.255.0
#
return
```

   - 如果接口下配置了 **undo fr inarp**，说明当前接口下禁用了 InARP，则执行 **fr inarp** 命令使能 InARP。
   - 如果接口下 InARP 已经使能，则进行步骤 5。

5. 检查两端是否都生成了 map

   执行 **display fr map-info** 命令，查看是否生成了对接设备 FR 接口 IP 地址的 MAP。

```
[Huawei-Serial2/0/0:2]display fr map-info
Map Statistics for interface MFR0/0/0 (DCE)
  DLCI = 100, bridge 1, MFR0/0/0
    create time = 2008/01/03 18:25:22, status = ACTIVE
    encapsulation = ietf, vlink = 0, broadcast
Map Statistics for interface Serial2/0/0:2 (DTE)
  DLCI = 300, IP INARP 7.7.7.1, Serial2/0/0:2
    create time = 2008/01/04 15:19:45, status = ACTIVE
    encapsulation = ietf, vlink = 9, broadcast
```


版权所有 © 华为技术有限公司

- 如果未生成 map，则重新进行配置。
- 如果已经生成了 map，则执行步骤 6。

6. 检查两端是否生成路由

执行 **display fib** 命令查看路由表，

```
[Huawei-Serial2/0/0:0]display this
[V200R001C00B130]
#
interface Serial2/0/0:0
 link-protocol fr
 fr interface-type dce
 fr dlci 22
 ip address 7.7.7.2 255.255.255.0
#
return
[Huawei-Serial2/0/0:0]display fib
Route Flags: G - Gateway Route, H - Host Route,    U - Up Route
             S - Static Route,  D - Dynamic Route, B - Black Hole Route
------------------------------------------------------------------------------
 FIB Table:
 Total number of Routes : 17

Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
7.7.7.1/32         7.7.7.1         HU   t[2917]       S2/0/0:0        0x0
7.7.7.255/32       127.0.0.1       HU   t[2907]       InLoop0         0x0
7.7.7.2/32         127.0.0.1       HU   t[2907]       InLoop0         0x0
50.1.1.255/32      127.0.0.1       HU   t[2519]       InLoop0         0x0
50.1.1.1/32        127.0.0.1       HU   t[2519]       InLoop0         0x0
192.168.0.255/32   127.0.0.1       HU   t[495]        InLoop0         0x0
192.168.0.23/32    127.0.0.1       HU   t[495]        InLoop0         0x0
36.1.1.255/32      127.0.0.1       HU   t[492]        InLoop0         0x0
36.1.1.2/32        127.0.0.1       HU   t[492]        InLoop0         0x0
255.255.255.255/32 127.0.0.1       HU   t[484]        InLoop0         0x0
127.255.255.255/32 127.0.0.1       HU   t[484]        InLoop0         0x0
127.0.0.1/32       127.0.0.1       HU   t[484]        InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[484]        InLoop0         0x0
36.1.1.0/24        36.1.1.2        U    t[492]        VT3             0x0
192.168.0.0/24     192.168.0.23    U    t[495]        GE0/0/0         0x0
50.1.1.0/24        50.1.1.1        U    t[2519]       S2/0/1:15       0x0
7.7.7.0/24         7.7.7.2         U    t[2907]       S2/0/0:0        0x0
```

如上显示信息，本端 IP 地址为：7.7.7.2，对端 IP 地址为 7.7.7.1。加粗的路由条目为生成的正确的路由表项。

- 如果不存在如上所示正确的路由条目，则重新配置路由。
- 如果路由表项正确，则进行步骤 7。

7. 请收集如下信息，并联系华为技术支持工程师。
   - 上述步骤的执行结果。
   - 设备的配置文件、日志信息、告警信息。

- PVC-Group 场景诊断步骤

1. 检查两端 PVC-Group 状态是否为 Active

   执行 **display fr pvc-group** 命令，查看 PVC-Group 状态。

```
[Huawei-Serial2/0/0:0]display fr pvc-group
PVC-GROUP-name    State     TosType     INARP   Interface        Type PhyStatus
1                   Active    PRECEDENCE  Enable  Serial2/0/0:0    DTE  Up
```

   - 如果显示信息中 PVC-Group 状态不是 Active，请重新检查接口物理状态。
   - 如果显示信息中 PVC-Group 状态是 Active，则进行步骤 2。

2. 检查 PVC-Group 内所有优先级是否分配完全

版权所有 © 华为技术有限公司

在接口视图下执行 **display this** 命令，查看接口下的配置。

```
[Huawei-Serial2/0/0:0]display this
interface Serial2/0/0:0
 link-protocol fr
 fr pvc-group 1
  fr dlci 22
  fr dlci 33
  fr ip precedence 22 0 4
  fr ip precedence 33 default
 ip address 7.7.7.2 255.255.255.0
#
return
```

说明

IP 报文的优先级有 precedence 和 dscp 两种，precedence 有 0~7 共 8 个级别，dscp 有 0~63 共 64 个级别。在未配置缺省 pvc 的场景下，需要将所有级别分配到 pvc-group 下的 pvc 上。

- 如果 PVC-Group 的优先级未分配完全，则重新配置。
- 如果 PVC-Group 的优先级已分配完全，则进行步骤 3。

3. 请收集如下信息，并联系华为技术支持工程师。
   - 上述步骤的执行结果。
   - 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

FR 协议 UP/Down 时会出现如下告警：

FR/4/TRAP:OID 1.3.6.1.2.1.10.32.0.1 Interface 9 DLCI 22 turns into 2 state (invalid(1), active (2),inactive(3)).

%%01IFNET/4/LINK_STATE(l)[3]:The line protocol on the interface Serial1/0/0:0 has entered the UP state.

相关日志

无

5.2.2 故障案例

一端 IP 地址未配置导致 FR 链路协议 UP 但无法 ping 通

网络环境

在如图 5-4 的网络中，两台 AR2200-S 通过 CE1 接口板直连。FR 链路协议 UP，但无法互相 Ping 通。

版权所有 © 华为技术有限公司

图 5-4 FR 链路直连设备无法相互 ping 通组网图

故障分析

1. 检查 DCE 侧是否配置 PVC。
2. 检查 DTE 侧接口下是否有 PVC。
   执行 **display fr pvc-info** 查看 DTE 是否有 PVC。
3. 检查 DTE 侧接口下 IP 地址配置是否正确。
   检查发现接口下未配置 IP 地址。

操作步骤

步骤 1 在 DTE 接口下配置 IP 地址。

完成步骤 1 后，两台 Huawei AR2200-S 系列可以相互 Ping 通。

----结束

案例总结

FR 链路协议 UP 后，DTE 会通过 LMI 向 DCE 学习 PVC。接口下配置 IP 地址后，DTE 和 DCE 会在接口下的 PVC 上用 InArp 学习对端的 IP 地址，进而生成路由表项。正确生成路由表项，才可以 Ping 通对端。

5.3 MFR 故障处理

5.3.1 MFR 链路协议 UP，但无法 ping 通对端的定位思路

常见原因

PING 操作分为直连 PING 和转发 PING 两种。

本类故障的常见原因包括：

- 基本 MFR 场景
  1. 接口下未配置 IP 地址
  2. 未生成 Map
  3. 生成 Map，但未生成路由

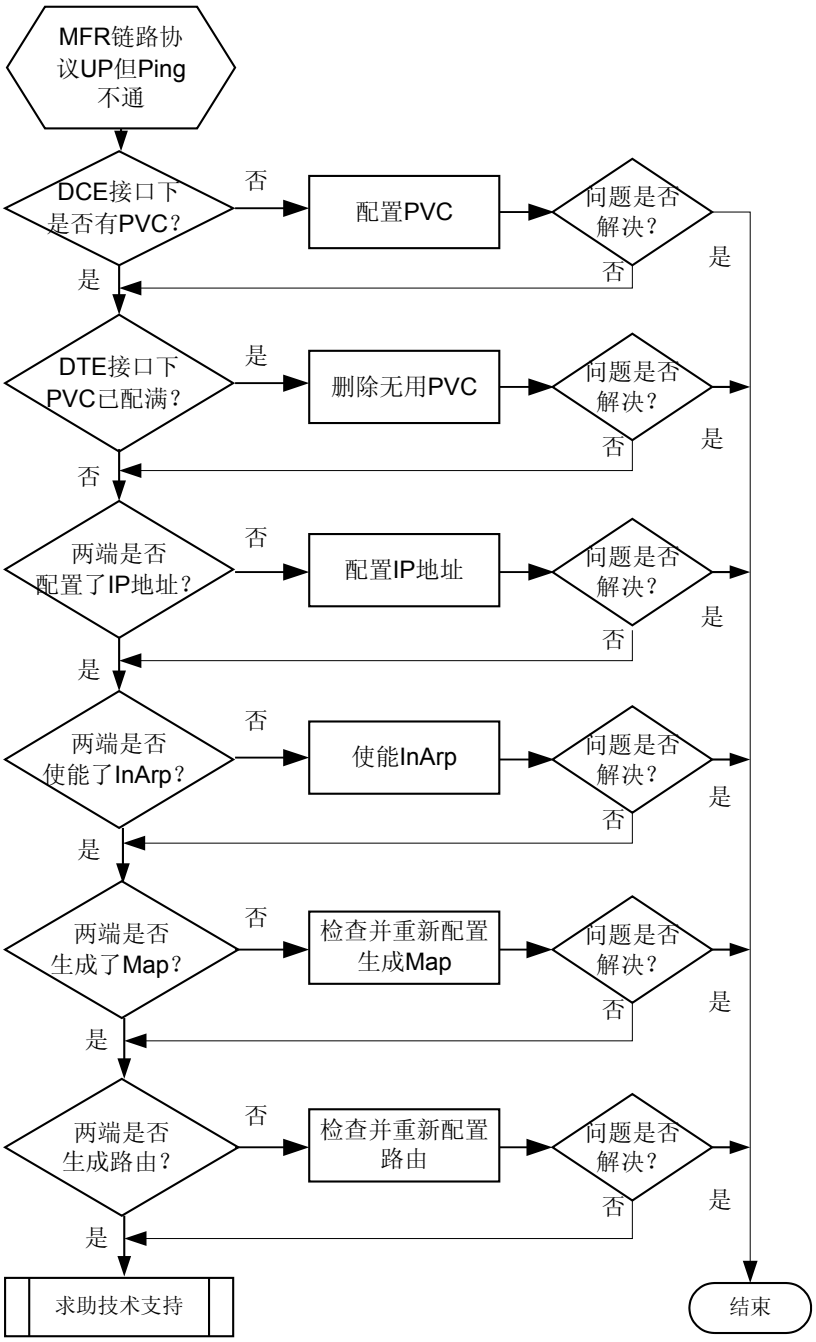
版权所有 © 华为技术有限公司

- PPPoMFR 场景
  1. Vrtual-template 中没有配置 IP
  2. PPP 协商失败

故障诊断流程

基本 MFR 场景详细故障处理流程，如图 5-5 所示。

图 5-5 MFR 链路协议 UP 但 PING 不通故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

- MFR 场景诊断步骤
  1. 检查 DTE 侧接口下是否有 PVC

     在系统视图下执行 **display fr pvc-info interface Serial** 命令，查看 PVC 状态。

```
[Huawei-MFR0/0/0]display fr pvc-info  interface  MFR
0/0/0
PVC statistics for interface MFR0/0/0 (DTE, physical
UP)
    DLCI = 22, USAGE = UNUSED (00000000),
MFR0/0/0
    create time = 2007/11/28 12:14:44, status =
ACTIVE
    InARP = Enable, PVC-GROUP =
NONE
    in packets = 22, in bytes =
994
    out packets = 22, out bytes = 950
```

     - 如果显示信息中无 PVC 信息，则说明该接口下没有 PVC，请重新在 DCE 侧进行 PVC 配置，或者在 DTE 侧进行 PVC 配置，且确保 DCE 侧配置了 PVC。
     - 如果显示信息中 **status** 字段值为 **INACTIVE**，可能 DCE 侧没有配置 PVC，请重新在 DCE 侧进行 PVC 配置。
     - 如果显示信息中 **status** 字段值为 **ACTIVE**，则说明 PVC 正常，请进行步骤 2。

     说明

     若 DTE 侧使用的是子接口，需要手动在子接口上配置 DLCI。

  2. 查看 DTE 侧的 PVC 是否已经配满

     执行 **display fr pvc-info** 命令，查看当前已有的 PVC。

```
[Huawei-MFR0/0/0]display fr pvc-
info
PVC statistics for interface MFR0/0/0 (DTE, physical
UP)
    DLCI = 22, USAGE = UNUSED (00000000),
MFR0/0/0
    create time = 2007/11/28 12:14:44, status =
ACTIVE
    InARP = Enable, PVC-GROUP =
NONE
    in packets = 29, in bytes =
1218
    out packets = 29, out bytes = 1160
```

     如果显示信息中，现有的 PVC 个数已经达到产品的规格限制，就不能再创建 PVC 了。AR2200-S 支持的 PVC 规格上限为 128。

     - 如果因为 PVC 超过规格无法创建，导致 PING 不通，则需要执行命令 **undo fr dlci dlci-number** 命令将无用的 PVC 删除。

版权所有 © 华为技术有限公司

- 如果 PVC 未超过规格，则进行步骤 3。

说明

只有在 DCE 和 DTE 侧都删除 dlci 才是有效的。

3. 检查两端设备的接口下是否都配置了 IP 地址

在 MFR 接口视图下执行 **display this** 命令，查看此接口下是否配置了 IP 地址。

```
[Huawei-MFR0/0/0]display this
[
V200R001C00B130]

#

interface
MFR0/0/0

 ip address 5.5.5.2 255.255.255.0
```

- 如果接口下未配置 IP 地址，则在接口下进行配置。
- 如果接口下已经配置了 IP 地址，则进行步骤 4。

4. 检查接口下是否使能了 InARP

执行 **display this** 命令，查看当前接口下的配置。

```
[Huawei-Serial2/0/0:2]display this
[
V200R001C00B130]

#

interface
MFR0/0/0

 undo fr
inarp

 ip address 5.5.5.2
255.255.255.0

#

return
```

- 如果接口下配置了 **undo fr inarp**，说明当前接口下禁用了 InARP，则执行 **fr inarp** 命令使能 InARP。
- 如果接口下 InARP 已经使能，则进行步骤 5。

5. 检查两端是否都生成了 map

执行 **display fr map-info** 命令，查看是否生成了对接设备 MFR 接口 IP 地址的 MAP。

```
[Huawei]display fr map-info
Map Statistics for interface MFR0/0/0
(DTE)
  DLCI = 22, IP INARP 5.5.5.1,
MFR0/0/0
    create time = 2007/11/28 14:04:21, status =
ACTIVE
    encapsulation = ietf, vlink = 2, broadcast
```

- 如果未生成 map，则重新进行配置。
- 如果已经生成了 map，则执行步骤 6。

版权所有 © 华为技术有限公司

6. 检查两端是否生成路由

执行 **display fib** 命令查看路由表，

```
[Huawei-MFR0/0/0]display this
#

interface
MFR0/0/0

 ip address 5.5.5.2
255.255.255.0

return
[Huawei-MFR0/0/0]display fib
Route Flags: G - Gateway Route, H - Host Route,    U - Up
Route
             S - Static Route,  D - Dynamic Route, B - Black Hole
Route
------------------------------------------------------------------------------

 FIB
Table:

 Total number of Routes :
17


Destination/Mask   Nexthop         Flag TimeStamp     Interface
TunnelID
5.5.5.1/32         5.5.5.1         HU   t[2082]       MFR0/0/0
0x0
5.5.5.255/32       127.0.0.1       HU   t[1025]       InLoop0
0x0
5.5.5.2/32         127.0.0.1       HU   t[1025]       InLoop0
0x0
50.1.1.255/32      127.0.0.1       HU   t[545]        InLoop0
0x0
50.1.1.1/32        127.0.0.1       HU   t[545]        InLoop0
0x0
192.168.0.255/32   127.0.0.1       HU   t[501]        InLoop0
0x0
192.168.0.23/32    127.0.0.1       HU   t[501]        InLoop0
0x0
6.6.6.255/32       127.0.0.1       HU   t[496]        InLoop0
0x0
6.6.6.2/32         127.0.0.1       HU   t[496]        InLoop0
0x0
255.255.255.255/32 127.0.0.1       HU   t[487]        InLoop0
0x0
127.255.255.255/32 127.0.0.1       HU   t[487]        InLoop0
0x0
127.0.0.1/32       127.0.0.1       HU   t[487]        InLoop0
0x0
127.0.0.0/8        127.0.0.1       U    t[487]        InLoop0
0x0
6.6.6.0/24         6.6.6.2         U    t[496]        VT3
0x0
192.168.0.0/24     192.168.0.23    U    t[501]        GE0/0/0
0x0
50.1.1.0/24        50.1.1.1        U    t[545]        S2/0/1:23
0x0
5.5.5.0/24         5.5.5.2         U    t[1025]       MFR0/0/0
0x0
```

如上显示信息，本端 IP 地址为：5.5.5.2，对端 IP 地址为 5.5.5.1，该路条目为生成的正确的路由表项。

- 如果不存在如上所示正确的路由条目，则重新配置路由。

版权所有 © 华为技术有限公司

- 如果路由表项正确，则进行步骤 7。

7. 请收集如下信息，并联系华为技术支持工程师。
   - 上述步骤的执行结果。
   - 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

MFR 协议 UP/Down 时会出现如下告警：

FR/4/TRAP:OID 1.3.6.1.2.1.10.32.0.1 Interface 9 DLCI 22 turns into 2 state (invalid(1), active (2),inactive(3)).

%%01IFNET/4/LINK_STATE(l)[9]:The line protocol on the interface MFR0/0/0 has entered the UP state

%%01IFNET/4/LINK_STATE(l)[11]:The line protocol PPP IPCP on the interface Virtual-Template3:0 ha s entered the UP state.

相关日志

无

5.3.2 故障案例

一端 InARP 未配置，导致 MFR 链路协议 UP 但无法 ping 通

网络环境

在如图 5-6 的网络中，两台 Huawei AR2200-S 系列通过 CE1 接口板直连。MFR 链路协议 UP，但无法互相 Ping 通。

图 5-6 FR 链路直连设备无法相互 ping 通组网图

故障分析

1. 检查 DCE 侧是否配置 PVC。
   发现 InARP 被禁用。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 启用 InARP。

完成步骤 1 后，两台 Huawei AR2200-S 系列可以相互 Ping 通。

----结束

案例总结

FR 链路协议 UP 后，DTE 会通过 LMI 向 DCE 学习 PVC。接口下配置 IP 地址后，DTE 和 DCE 会在接口下的 PVC 上用 InARP 学习对端的 IP 地址，进而生成路由表项。正确生成路由表项，才可以 Ping 通对端。

5.4 DCC 故障处理

5.4.1 ISDN 拨号不通的定位思路（发起呼叫）

常见原因

本类故障的常见原因主要包括：

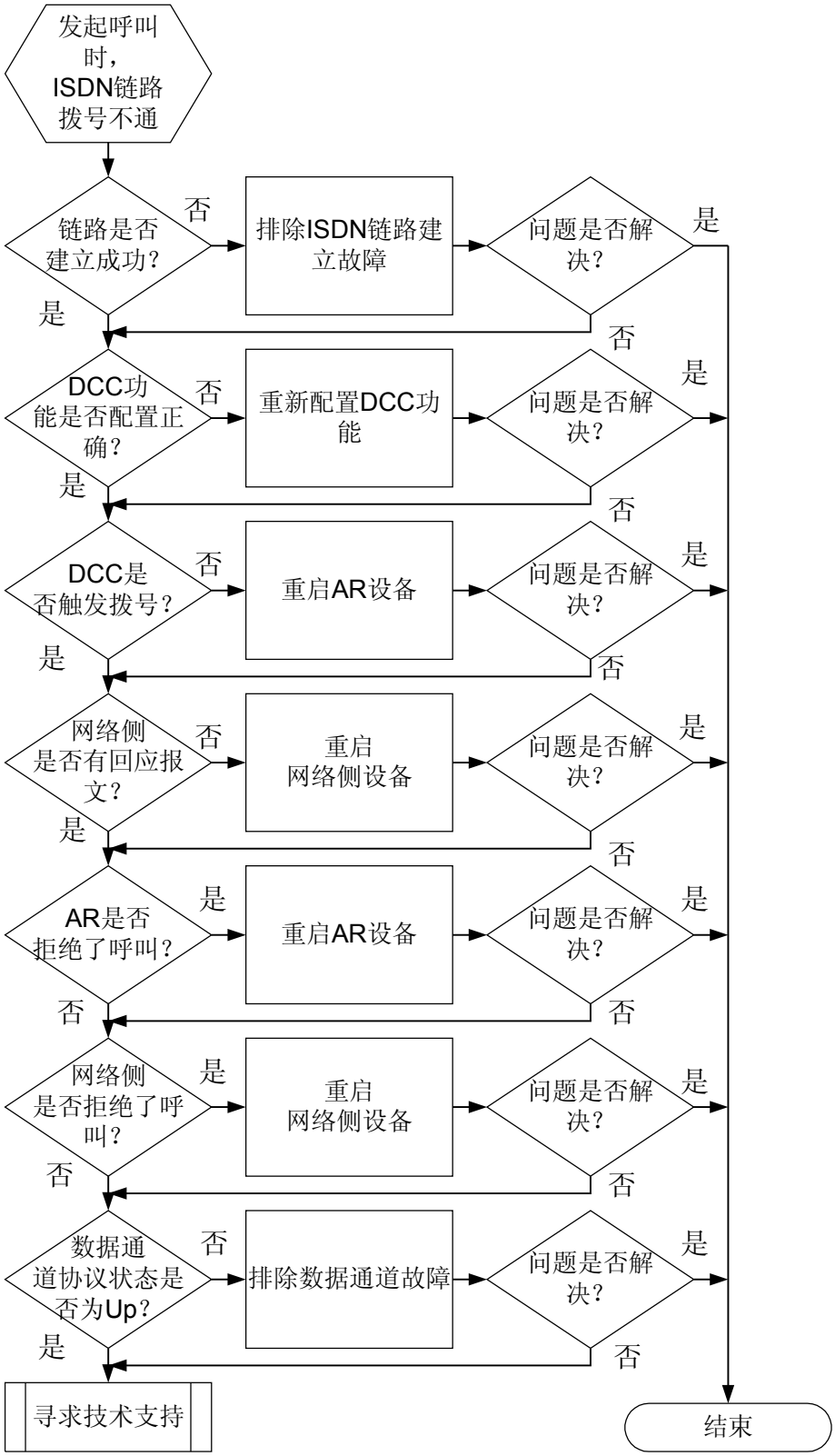
- 链路建立失败的各种原因
- DCC 拨号功能配置有误，无法触发拨号
- 网络侧设备出现故障，无法回应正确的交互报文
- 交互的报文有误，导致 AR 拒绝了呼叫
- 交互的报文有误，导致网络侧设备拒绝了呼叫
- 数据通道协议协商失败，导致通道无法 UP

故障诊断流程

详细处理流程如图 5-7 所示。

版权所有 © 华为技术有限公司

图 5-7 ISDN 拨号不通（发起呼叫）故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查链路是否建立成功

执行 **display isdn call-info** 命令，查看呼叫状态。

- 如果无任何显示信息，说明 PRI 接口没有被创建，请配置相应的 PRI 接口。
- 如果显示信息中包含“State = TEI_ASSIGNED”或者“State = AWAITING_ESTABLISHMENT”说明链路建立失败，请参考 **5.5.1 ISDN 接口建立链路失败的定位思路**。
- 如果显示信息中包含“State = MULTIPLE_FRAME_ESTABLISHED ”说明链路建立成功，请执行步骤 2。

步骤 2 检查 DCC 拨号功能配置是否正确

进入 Serial 接口视图或者 Dialer 接口视图后执行 **display this** 命令，查看当前接口的配置信息。检查以下配置是否正确。

- 是否配置了 dialer-rule，并且 Dialer-rule number 和 Dialer-group number 一致。
- 当采用 dialer number 方式拨号时，dialer number 是否正确。
- 当采用 dialer route ip 方式拨号时，ip 地址是否正确。

说明

对于 Serial 接口，可以通过执行 **diaplay device** 命令检查“2E1/T1-M”所在的槽位号，获取 Serial 的接口的槽位号。

如果上述信息有配置错误，请重新配置 DCC 拨号功能，如果上述信息配置均正确，请依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，检查 DCC 是否触发了拨号。

- 如果显示信息中，没有任何 DCC 调试信息，表明 DCC 没有触发拨号，需要重启设备。
- 如果显示信息中，存在 DCC 调试信息，表明 DCC 触发了拨号，但是不一定拨号成功，请执行步骤 3。

开启调试开关后，当 DCC 触发拨号时的 Debugging 信息如下所示：

```
<Huawei>
Oct 14 2007 09:07:40.760.1+08:00 AR2220 DCC/7/debug:DCC: try to find routing to '4.4.4.2' on
interface Dialer1
Oct 14 2007 09:07:40.760.2+08:00 AR2220 DCC/7/debug:DCC: the packet is interesting.
Oct 14 2007 09:07:40.760.3+08:00 AR2220 DCC/7/debug:DCC: DCC_ProcPktForDialNum called...
Oct 14 2007 09:07:40.760.4+08:00 AR2220 DCC/7/debug:DCC: DCC_ProcDialPktNoLink: Dial to the remote
host
Oct 14 2007 09:07:40.770.1+08:00 AR2220 DCC/7/debug:DCC: Try to find a free channel to dial
'01234567890123456789012345678 9' on the interface Dialer1
Oct 14 2007 09:07:40.770.2+08:00 AR2220 DCC/7/debug:DCC: Dialing 01234567890123456789012345678 9 on
interface Serial1/0/0:15 of interface Dialer1
Oct 14 2007 09:07:40.770.3+08:00 AR2220 DCC/7/debug:DCC: DDR Dial :send DDR_CONN_REQ message
successfuly,sertype=8,IfIndex=0x9
Oct 14 2007 09:07:40.770.4+08:00 AR2220 DCC/7/debug:DCC: not set the queue! discard this packet
Oct 14 2007 09:07:40.780.1+08:00 AR2220 CC/7/
CC_Debug:
```


版权所有 © 华为技术有限公司

```
CC<-DDR :
ISDN_CONN_REQ

 CallID=0xffffffff UserID=0x2 PortID=0x9 ServiceType=0x8 Channel=0x2 IsCompleted=0x0 Cause=0x00
szCalledNum=012345678901234567894567 89
```

步骤 3 检查网络侧是否有回应报文

依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，检查网络侧是否有回应报文。

- 如果显示信息中，没有任何 N->U 的调试信息，说明网络侧没有回应报文，需要重启网络侧设备。
- 如果显示信息中，存在 N->U 的调试信息，说明网络侧有回应报文，请执行步骤 4。

步骤 4 检查 AR2200-S 是否拒绝了呼叫

ISDN 呼叫建立过程中，需要交互好几种不同的报文。在交互过程中，如果 AR2200-S 接收到不符合要求的报文，会主动拒绝此次呼叫。

依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，检查 AR2200-S 是否拒绝了呼叫。

- 如果有以下显示信息，表明 AR2200-S 拒绝了呼叫，需要重启 AR2200-S。

```
<Huawei> Oct 14 2007 08:56:10.30.1+08:00 AR2220 CC/7/CC_Debug:
CC <-DDR : ISDN_DISC_REQ
CallID=0x0 UserID=0x0 PortID=0x9 ServiceType=0x8 Channel=0x2 IsCompleted=0x0 Cause=0x00
Oct 14 2007 08:56:10.30.2+08:00 AR2220 CC/7/CC_Debug:
CC->Q931: PRIM_DISCONNECT_REQ
 CCIndex=0x0 L3Index=0x1 PortID=0x9 CES=0x1 *cause=08 02 80 90
Oct 14 2007 08:56:10.40.1+08:00 AR2220 Q931/7/Q931_Debug: Serial1/0/0:15
    U->N   DL_I_Data_Req  CES = 1
    cr= 01 01 DISCONNECT  *cause=08 02 80 90
```

- 如果显示信息中，没有以上信息，表明 AR2200-S 没有拒绝呼叫，请执行步骤 5。

步骤 5 检查网络侧是否拒绝了呼叫

依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，检查网络侧是否拒绝了呼叫。

- 如果显示信息，表明网络侧拒绝了呼叫，需要重启网络侧设备。

```
<Huawei> Oct 14 2007 09:40:38.10.1+08:00 AR2220 Q931/7/Q931_Debug: Serial1/0/0:15
    N->U   DL_I_Data_Ind  CES = 1
    cr= 01 84 DISCONNECT  *cause=08 02 80 90
Oct 14 2007 09:40:38.10.2+08:00 AR2220 Q931/7/Q931_Debug:
 [FUN: ProcMsgDisconnect, LINE: 545] ISDN Layer 3 call state change:->
CS_DISCONNECT_INDICATION
Oct 14 2007 09:40:38.10.3+08:00 AR2220 CC/7/CC_Debug:
CC<-Q931: PRIM_DISCONNECT_IND
 CCIndex=0x3 L3Index=0x4 PortID=0x9 CES=0x1 *cause=08 02 80 90
```

- 如果显示信息中，没有以上信息，表明网络侧没有拒绝呼叫，请执行步骤 6。

步骤 6 检查数据通道协议是否 Up

执行 **display isdn active-channel** 命令，查看当前激活的数据通道。

```
<Huawei> display isdn active-channel
Serial1/0/0:15
--------------------------------------------------------------------------------
Channel  Call     Call     Calling        Calling     Called         Called
Info     Property Type     Number         Subaddress Number         Subaddress
--------------------------------------------------------------------------------
B26      Digital  Out      88888204           -        88888206          -
```


版权所有 © 华为技术有限公司

执行 **display interface serial 1/0/0:15**，查看当前呼叫所对应的数据通道信息。如果协议的状态显示为“Line protocol current state : UP ”说明数据通道协议已经 Up。请执行步骤 7。

如果协议的状态显示为“Line protocol current state : DOWN”说明数据通道协议状态为 DOWN。请参考 PPP 接口协议 Down 的定位思路。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

5.4.2 ISDN 拨号不通的定位思路（接受呼叫）

常见原因

本类故障的常见原因主要包括：

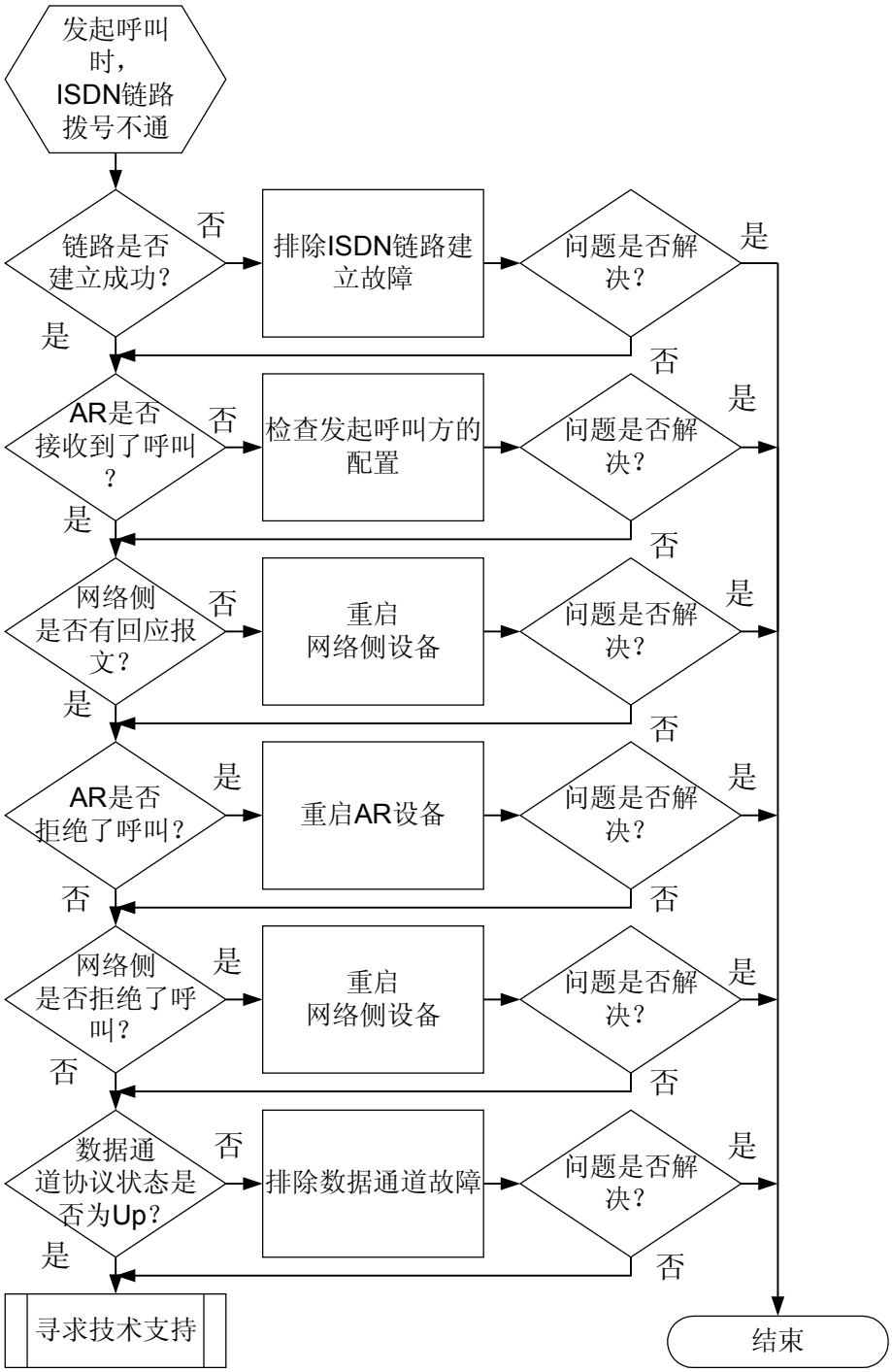
- 链路建立失败的各种原因
- AR 未接收到呼叫
- 呼叫信息有误，导致 AR 拒绝了呼叫
- 呼叫信息有误，导致网络侧设备拒绝了呼叫
- 数据通道协议协商失败，导致通道无法 UP

故障诊断流程

详细处理流程如图 5-8 所示。

版权所有 © 华为技术有限公司

图 5-8 ISDN 拨号不通（接受呼叫）故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查链路是否建立成功

执行 **display isdn call-info** 命令，查看呼叫状态。

- 如果无任何显示信息，说明没有 PRI 接口没有被用作拨号接口，请重新配置拨号功能。
- 如果显示信息中包含“State = TEI_ASSIGNED”或者“State = AWAITING_ESTABLISHMENT”说明链路建立失败，请参考“ISDN 接口建立链路失败的定位思路”。
- 如果显示信息中包含“State = MULTIPLE_FRAME_ESTABLISHED ”说明链路建立成功，请执行步骤 2。

步骤 2 检查 AR2200-S 是否接收到呼叫

依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，查看设备发送和接收的报文。

- 如果调试信息中，没有任何 N->U 的调试信息，说明 AR2200-S 没有接收到呼叫，请检查发起呼叫方的配置。
- 如果显示以下信息，表明 AR2200-S 接收到了呼叫。请执行步骤 3。

```
<Huawei>
Oct 14 2007 10:30:19.160.1+08:00 AR2220 Q931/7/Q931_Debug:
Serial1/0/0:15
    N->U   DL_I_Data_Ind  CES =
1                                                                    cr= 02 00 e7
SETUP  *send_comp=a1 *bearer=04 02 88 90 *chan_id=18 03 a1 83 9a *called_n=70 05 80 30 31 32
33
```

步骤 3 检查 AR2200-S 是否拒绝了呼叫

ISDN 呼叫建立过程中，需要交互几种不同的报文。在交互过程中，如果 AR2200-S 接收到不符合要求的报文，会主动拒绝此次呼叫。

依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，检查 AR2200-S 是否拒绝了呼叫。

- 如果显示以下信息，表明 AR2200-S 拒绝了呼叫，需要重启 AR。

```
<Huawei> Oct 14 2007 08:56:10.30.1+08:00 AR2220 CC/7/CC_Debug:
CC <-DDR : ISDN_DISC_REQ
CallID=0x0 UserID=0x0 PortID=0x9 ServiceType=0x8 Channel=0x2 IsCompleted=0x0 Cause=0x00
Oct 14 2007 08:56:10.30.2+08:00 AR2220 CC/7/CC_Debug:
CC->Q931: PRIM_DISCONNECT_REQ
 CCIndex=0x0 L3Index=0x1 PortID=0x9 CES=0x1 *cause=08 02 80 90
Oct 14 2007 08:56:10.40.1+08:00 AR2220 Q931/7/Q931_Debug: Serial1/0/0:15
    U->N   DL_I_Data_Req  CES = 1
    cr= 01 01 DISCONNECT  *cause=08 02 80 90
```

- 如果显示信息中，没有以上信息，表明 AR2200-S 没有拒绝呼叫，请执行步骤 4。

步骤 4 检查网络侧是否拒绝了呼叫

ISDN 呼叫建立过程中，需要交互几种不同的报文。在交互过程中，如果网络侧接收到不符合要求的报文，会拒绝此次呼叫。

依次执行 **debugging dialer all**，**debugging isdn cc**，**debugging isdn q931**，**terminal debugging**，**terminal monitor** 命令，检查网络侧是否拒绝了呼叫。

- 如果显示信息，表明网络侧拒绝了呼叫，需要重启网络侧设备。

版权所有 © 华为技术有限公司

```
<Huawei> Oct 14 2007 09:40:38.10.1+08:00 AR2220 Q931/7/Q931_Debug: Serial1/0/0:15
    N->U   DL_I_Data_Ind  CES =
1
    cr= 01 84 DISCONNECT  *cause=08 02 80 90
Oct 14 2007 09:40:38.10.2+08:00 AR2220 Q931/7/
Q931_Debug:
 [FUN: ProcMsgDisconnect, LINE: 545] ISDN Layer 3 call state change:->
CS_DISCONNECT_INDICATION
Oct 14 2007 09:40:38.10.3+08:00 AR2220 CC/7/
CC_Debug:
CC<-Q931:
PRIM_DISCONNECT_IND
 CCIndex=0x3 L3Index=0x4 PortID=0x9 CES=0x1 *cause=08 02 80 90
```

- 如果显示信息中，没有以上信息，表明网络侧没有拒绝呼叫，请执行步骤 5。

步骤 5 检查数据通道协议是否 Up

执行 **display isdn active-channel** 命令，查看当前激活的数据通道。

```
<Huawei> display isdn active-
channel

Serial1/0/0:15

-------------------------------------------------------------------------------

Channel  Call     Call     Calling        Calling     Called
Called
Info     Property Type     Number         Subaddress Number
Subaddress
-------------------------------------------------------------------------------

B26      Digital  Out      88888204           -       88888206          -
```

执行 **display interface serial 1/0/0:15**，查看当前呼叫所对应的数据通道信息。如果协议的状态显示为“Line protocol current state : UP ”说明数据通道协议已经 Up。请执行步骤 6。

如果协议的状态显示为“Line protocol current state : DOWN”说明数据通道协议状态为 DOWN。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

5.5 ISDN 故障处理

版权所有 © 华为技术有限公司

5.5.1 ISDN 接口建立链路失败的定位思路

常见原因

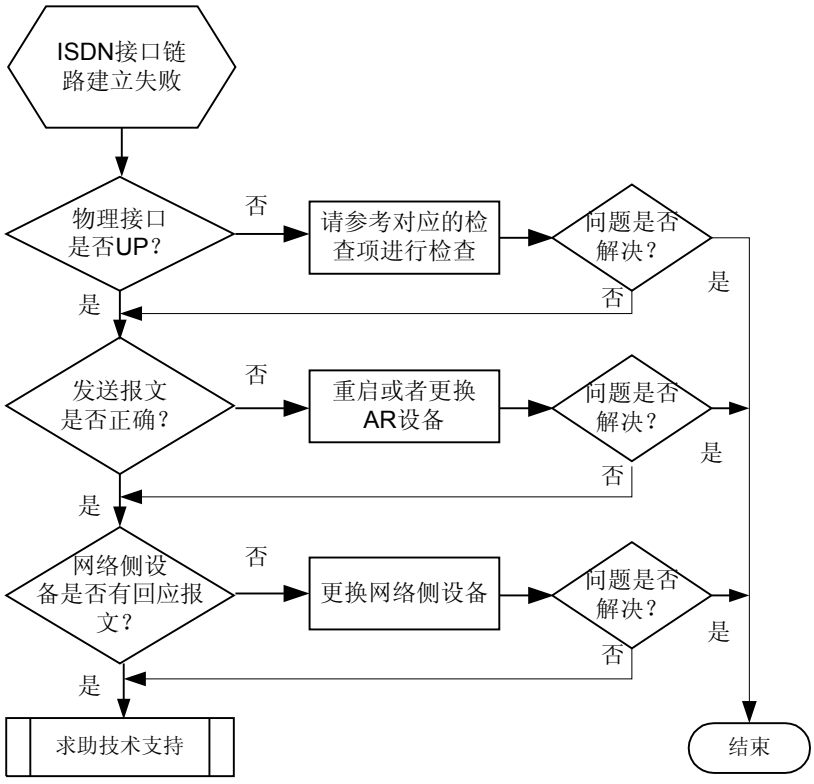
本类故障的常见原因主要包括：

- 对接线缆有问题
- 接口配置错误
- 报文处理出现了错误
- 网络侧设备出现故障

故障诊断流程

详细故障处理流程，如图 5-9 所示。

图 5-9 ISDN 接口建立链路失败故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查设备物理接口是否 Up

在系统视图下执行 **display controller E1** 命令查看接口物理状态是否 Up。这里以查看 E1 1/0/0 接口状态为例。

- 如果接口状态显示信息为“E1 1/0/0 current state : Administratively DOWN”，表示接口被 **shutdown**，请先在接口下执行 **undo shutdown** 命令开启接口。执行 **undo shutdown** 命令后如果接口的状态信息为“E1 1/0/0 current state : DOWN”，请参考接口状态显示信息为“E1 1/0/0 current state : DOWN”时的检查项继续检查。
- 如果接口的状态显示信息为“E1 1/0/0 current state : DOWN”，请执行如下检查。

检查项	检查标准	后续操作
检查本端和对端接口缆连接是否正常，线缆或模块是否故障。	如果显示信息中“Alarm State:”字段对应信息为“Loss-of-Signal”，表示可能存在如下问题： 1. 设备两端线缆连接不好。 2. 设备接口故障。 3. 设备线缆中断。	重新连接线缆，如果重新连接线缆后故障依然存在请尝试更换线缆、接口模块或设备。
工作模式是否正确	“Work Mode”字段表示接口的工作模式。可能的取值为： ● E1 FRAMED：当接口工作在成帧方式时，会显示这个状态 ● E1 UNFRAMED：当接口工作在非成帧方式时，会显示这个状态。 ISDN 接口两端的工作模式必须是成帧方式。	如果接口两端的工作模式为非成帧方式，请在 CE1 接口视图下执行 **pri-set** 命令配置接口的工作方式为成帧方式。
接口两端帧格式是否一致	“Frame-format”字段表示接口的帧格式，可能的取值为： ● CRC4：表示接口的帧格式为复帧。 ● NO-CRC4：表示接口的帧格式为基本帧，又称双帧或奇偶帧。 接口两端的帧格式必须一致。	如果接口两端的帧格式不一致，请在 CE1 接口视图下执行 **frame-format** 命令重新配置接口的工作模式，使两端的帧格式一致。
接口的线路码型是否一致	“Line Code”字段表示接口的线路码型，取值为 HDB3。接口两端配置的线路码型必须一致。	如果对端设备的线路码型不是 HDB3，请修改对端的线路码型为 HDB3，使两端的线路码型一致。
时钟模式配置是否正确	当两台路由器的 CE1 接口直接相连时，必须使两端分别工作在线路时钟模式（slave）和内部时钟模式（master）。	如果接口两端配置的时钟模式不正确，请在 CE1 接口视图下执行 **clock** 命令重新配置时钟模式。

版权所有 © 华为技术有限公司

检查项	检查标准	后续操作
接口两端是否配置接口环回	在 CE1 接口视图下执行 **display this** 命令查看接口是否配置了环回,接口下如果出现了“loopback local”、“loopback payload”或“loopback remote”表示接口配置了环回。环回会导致接口一段 Up 一段 Down 的情况，在执行完通过环回检测链路和接口是否正常后请及时取消接口环回配置。 **说明** 在系统视图下执行 **display controller E1** 命令时，如果显示信息中“Alarm State:”字段对应信息为“Alarm-Indication-Signal”表示接口可能配置环回。	如果接口两端配置的环回，请在 CE1 接口视图下执行 **undo loopback** 取消接口环回。

执行上述操作后如果接口物理状态仍为“DOWN”，请执行步骤 4。

- 如果有“E1 1/0/0 current state : UP”信息证明接口状态为 Up，请执行步骤 2。

步骤 2 检查设备发送的报文是否正确

说明

在系统视图下执行 **display controller E1** 命令时，如果显示信息中“Alarm State:”字段对应信息为“Remote-Alarm-Indication”，表示可能本端发送或对端接收存在问题。

依次执行 **debugging isdn q921**、**terminal debugging** 和 **terminal monitor** 命令，查看设备发送的报文。其中“U->N”表示从用户侧到网络侧，“Len”表示 SABME 帧的长度。正确的 SABME 帧的长度为 3 字节，内容为“00 01 7F”或“02 01 7F”。

- 如果显示如下信息，说明发送的 SABME 帧的长度和内容有误，需要重启或更换设备。

```
<Huawei>
Oct 12 2007 11:54:42.240.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=7 00 01 7F  00 00 00 00
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 11:54:43.240.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=7 00 01 7F 00 00 00
00
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 11:54:44.240.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=7 00 01 7F 00 00 00
00
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
```

- 如果显示如下信息，说明设备发送的报文是正确的，请执行步骤 3。

```
<Huawei>
Oct 12 2007 11:54:42.240.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
```


版权所有 © 华为技术有限公司

```
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 11:54:43.240.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 11:54:44.240.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
```

步骤 3 检查网络侧是否有正确的回应报文

说明

在系统视图下执行 **display controller E1** 命令时，如果显示信息中“Alarm State:”字段对应信息为“Remote-Alarm-Indication”，表示可能本端发送或对端接收存在问题，如果“Alarm State:”字段对应信息为“Loss-of-Frame”表示对端发送可能出现故障。

依次执行 **debugging isdn q921**、**terminal debugging** 和 **terminal monitor** 命令，查看设备发送的报文。其中“N->U”表示网络侧到用户侧，如果收到对端的回应报文可以看到“N->U”的输出信息。

- 如果显示如下信息（只有 U->N 信息），说明网络侧没有回应报文，请检查网络侧设备是否存在故障。

```
<Huawei>
Oct 12 2007 14:28:51.430.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 14:28:52.430.1+08:00 Huawei Q921/7/
Q921_Debug:
 [FUN: ISDN_Q921_T200Out, LINE: 2182] ISDN Layer 2 link state change -> TEI_ASSIGNED
<Huawei>
Oct 12 2007 14:28:57.430.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 14:28:57.430.2+08:00 Huawei Q921/7/
Q921_Debug:
 [FUN: ISDN_Q921_HandleEstablishReq, LINE: 185] ISDN Layer 2 link state change ->
AWAITING_ESTABLISHMENT
<Huawei>
Oct 12 2007 14:29:00.430.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME
p=1
Q921/7/Q921_Debug:
 [FUN: ISDN_Q921_T200Out, LINE: 2182] ISDN Layer 2 link state change -> TEI_ASSIGNED
```

- 如果显示如下信息，说明网络侧有正确的回应报文，请执行步骤 4。

```
<Huawei>
Oct 12 2007 14:28:57.430.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 14:28:57.430.1+08:00 Huawei Q921/7/Q921_Debug:
```


版权所有 © 华为技术有限公司

```
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 14:28:57.430.1+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    U->N Len=3 00 01
7F
    U->N sapi=00 tei=00 c/r=0  SABME  p=1
<Huawei>
Oct 12 2007 13:55:20.680.2+08:00 Huawei Q921/7/Q921_Debug:
Serial1/0/0:15
    N->U Len=3 02 01
73
    N->U sapi=00 tei=00 c/r=1  UA  f=1
<Huawei>
Oct 12 2007 13:55:20.680.3+08:00 Huawei Q921/7/
Q921_Debug:
 [FUN: ISDN_Q921_HandleOnTEIAssign, LINE: 1054] ISDN Layer 2 link state change ->
MULTIPLE_FRAME_ESTABLISHED
```

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

5.6 PPPoE 故障处理

5.6.1 PPPoE 拨号失败定位思路

常见原因

PPPoE 可以应用为 PPPoE Client 和 PPPoE Server。

本类故障的常见原因主要包括：

- 配置错误
- 底层物理接口不停 Up、Down 震荡
- 认证不通过
- 客户端不能正常分配到地址

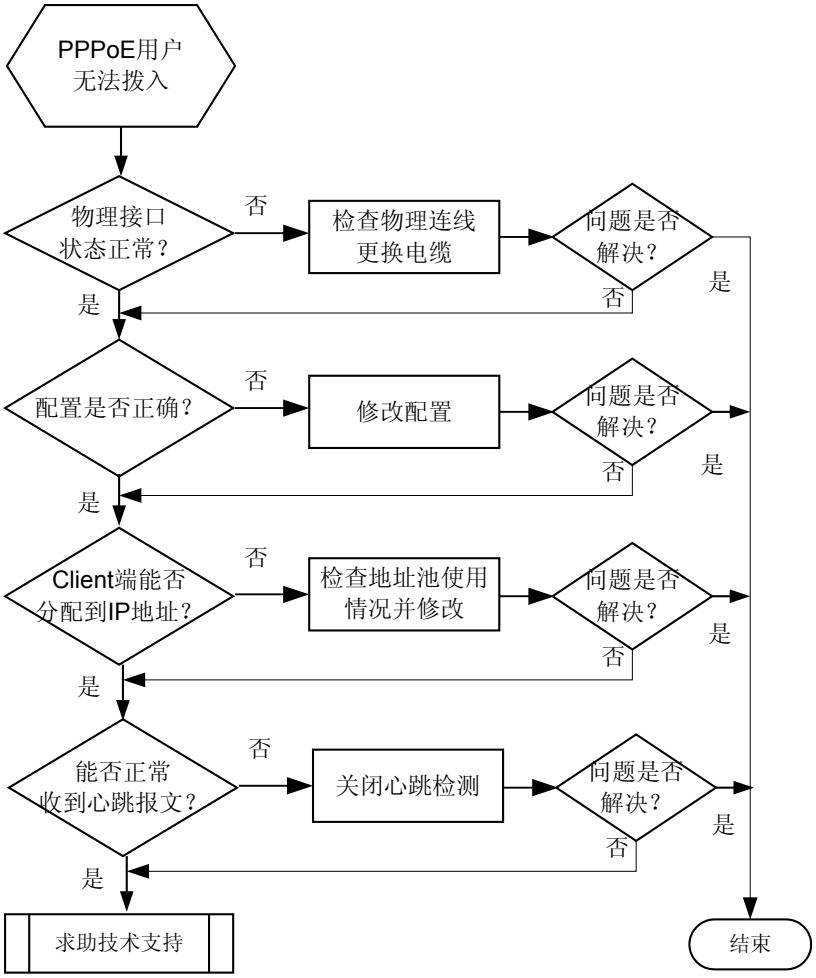
版权所有 © 华为技术有限公司

- 心跳报文没有正常收到

故障诊断流程

详细故障处理流程，如图 5-10 所示。

图 5-10 PPPoE 拨号失败故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查物理接口状态是否正常

在对应物理接口下执行 **display this interface** 命令，查看物理接口的状态是否不停的 Up/Down 震荡。

- 如果物理接口不停 UP/Down 震荡，则需检查物理连线或更换线缆。

版权所有 © 华为技术有限公司

- 如果端口状态正常，则执行步骤 2。

步骤 2 检查配置是否正确

如果是 Server 侧，需要检查 VT 接口和以太物理接口下的配置，如果是 Client 侧，需要检查 Dialer 接口和以太物理接口下的配置。在设备对应接口下执行 **display this** 命令，查看相应的配置。

Server 侧

```
[Huawei-A-Virtual-Template10]display this
ppp authentication-mode chap
[Huawei-A-aaa]display this
local-user ub password simple user1
```

Client 侧

```
[Huawei-B-Dialer10]display this
 ppp chap user ub
 ppp chap password simple ub
 dialer-group 5
[Huawei-B-GigabitEthernet0/0/1]display this
pppoe-client dial-bundle-number 10
[Huawei-B-dialer-rule]display this
dialer-rule
dialer-rule 5 ip permit
```

- 如果 Server 侧配置了认证，则需要确认 Client 侧是否配置了正确的用户名和密码。如果 Client 侧配置的是流量触发上线，则没有流量的时候拆链属于正常现象，并且需要注意在 dialer rule 模式下的 dialer-rule 后的拨号访问组编号要和 dialer 接口下的 dialer-group 后面的访问组编号一致。
- 如果配置均正确但故障仍旧存在，请执行步骤 3。

步骤 3 检查用户无法拨入的原因

对于 Client 侧，检查是否验证阶段不通过导致不停 Up/Down 震荡。执行如下命令，查看打印的具体信息，其中 Dialer 口为该连接的对应拨号口。

```
<Huawei-B>terminal monitor
Info: Current terminal monitor is on.
<Huawei-B>terminal debugging
Info: Current terminal debugging is on.
Info: Current terminal monitor is on.
<Huawei-B>debugging ppp all interface Dialer 10
```

如果打印信息中有如下信息，则说明认证不通过。

```
<Huawei-B>Jan 21 2008 17:40:56.420.1+08:00 AR1220-B MID_PPP/7/debug2:
  PPP Packet:
      Dialer10:0 Input  CHAP(c223) Pkt, Len 33
      State SendResponse, code FAILURE(04), id 2, len 29
      Message: Illegal User or password.
<Huawei-B>Jan 21 2008 17:42:37.520.4+08:00 AR1220-B MID_PPP/7/debug2:
  PPP Packet:
      Dialer10:0 Output LCP(c021) Pkt, Len 13
      State reqsent, code ConfRej(04), id 1, len 9
      AuthProto(3), len 5, CHAP c22305

<Huawei-B>Jan 21 2008 17:42:37.530.6+08:00 AR1220-B MID_PPP/7/debug2:
  PPP Packet:
      Dialer10:0 Input  LCP(c021) Pkt, Len 8
      State opened, code TermReq(05), id 3, len 4
```

以上三段打印信息，第一段意思是 Client 侧配置了 chap 用户名，接受对面 Server 端发送的 Challenge 并回应一个 Response，但是由于密码错误或者用户名密码不存在，Server 端发送了 Response 失败的消息。第二段意思是 Client 侧没有配置认证信息或配置的认证方式不一致，则直接拒绝了 Server 端 LCP 阶段的认证请求。超过 4 次之后，会触发收到第三段报文，即 Server 端发送终结链路请求。

版权所有 © 华为技术有限公司

- 如果认证失败，则检查认证配置并修改正确的认证用户名密码。
- 如果认证通过但故障仍旧存在，请执行步骤 4。

步骤 4 检查 Client 端能否正常分配到 IP 地址

如果 Client 端不能正确的分配到 IP 地址，则需要查看 Server 端的对应配置。如果是地址池方式分配远端地址，则需要确认地址池中是否还有可用地址。登录到 Server，键入如下命令查看相应信息。

```
[Huawei-A-ip-pool-mypoo]display ip pool name mypool
  Pool-name      : mypool
  Pool-No        : 0
  Lease          : 1 Days 0 Hours 0 Minutes
  Domain-name    : -
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Local           Status           : Unlocked
  Gateway-0      : 20.1.1.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
        Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
       20.1.1.1      20.1.1.254   253     1   252       0         0         0
 ------------------------------------------------------------------------------
```

如果 Idle 下面的数字为 0，则说明已经没有空闲的 IP 地址可用，则需要将 Server 端的 VT 接口下的地址池修改成有空闲地址的地址池。 另外，如果 Client 端协商到的 IP 地址和本地的其他地址冲突，也会出现 UpDown 震荡的情况。

- 如果 Server 端未正常分配 IP 地址，则检查地址池使用情况，修改地址池。
- 如果 Server 端能正常分配 IP 地址，请执行步骤 5。

步骤 5 检查 Client 端能否正常收到心跳报文

登录到 Client 端，执行如下命令，查看打印信息。

```
<Huawei-B>terminal monitor
Info: Current terminal monitor is on.
<Huawei-B>terminal debugging
Info: Current terminal debugging is on.
<Huawei-B>debugging ppp lcp all interface Dialer 10
```

如果打印信息中只有 Output 方向的 EchoRequest，没有 Input 方向的 EchoReply，则说明 Client 侧收不到心跳报文。

```
[Huawei-B]
Jan 21 2008 19:20:37.790.2+08:00 AR1220-B MID_PPP/7/debug2:
  PPP Packet:
      Dialer10:0 Output LCP(c021) Pkt, Len 12
      State opened, code EchoRequest(09), id c0, len 8
      Magic Number 0560b017
```

当 Client 端连续发送 4 个心跳报文没有响应后，即会拆除链路。无论 Client 端能否正常收到心跳报文，请执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

版权所有 © 华为技术有限公司

相关告警

无

相关日志

无

5.7 PPP 故障处理

5.7.1 PPP 接口协议 Down 的定位思路

常见原因

在接口上配置 PPP 协议以后，LCP 协商不成功导致接口协议 Down。

本类故障的常见原因主要包括：

- 链路两端接口上的 PPP 相关配置错误。
- 接口的物理层没有 Up。
- PPP 协议报文被丢弃。
- 链路存在环路。
- 检查链路延时是否影响上层业务。

故障诊断流程

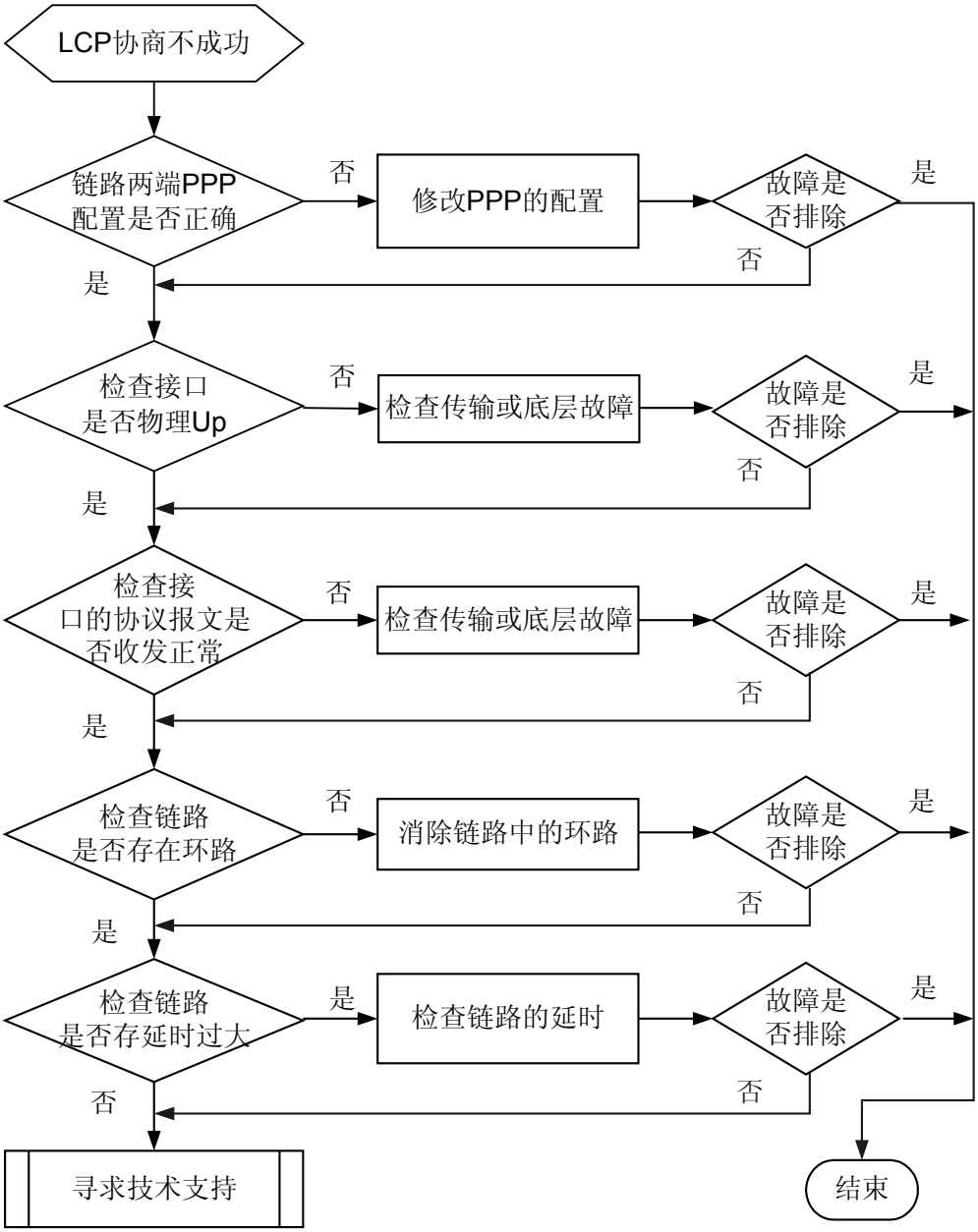
故障诊断思路：

- 检查链路两端的 PPP 相关配置错误。
- 检查接口是否物理 Up。
- 检查接口协议报文是否收发正常。
- 检查链路是否存在环路。
- 检查链路的延时是否过大。

可按照图 5-11 排除此类故障。

版权所有 © 华为技术有限公司

图 5-11 LCP 协商不成功故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查链路两端的 PPP 配置是否正确。

在协议 down 的接口视图下执行命令 **display this** 查看 PPP 相关配置。

```
[Huawei-Serial2/0/0] display this
#
interface Serial2/0/0
 link-protocol ppp
```


版权所有 © 华为技术有限公司

```
 undo shutdown
 ip address 10.10.1.1 255.255.255.0
#
return
```

- 检查如下两端对应的 PPP 相关的配置是否正确，如果不正确，请参考 PPP 的配置手册修改。
  - 确认认证及被认证类型保持一致，配置中 **ppp authentication-mode** *authentication-mode* 命令表示本端作为认证端所采用的认证模式，需要查看对端也就是被认证端所采用的认证模式，例如有 **ppp pap local-user** *user-name* **password simple** *password* 这个配置就表示被认证端采用的是 PAP 认证。
  - 确认两端是否进行了 MP 绑定，如果有一端绑定，则另外一端也需要绑定，或者两端都不绑定。配置中如果有 **ppp mp** *interface-type interface-number* 则说明此接口进行了 MP 绑定。
  - 判断被验证方和验证方的 PPP 认证配置的密码一致。
    - 认证模式为 PAP 模式的场景下用户名的及密码的查看方式如下：

      被验证方需要在接口视图下来查看用户名和密码。

      ```
      [Huawei-Serial2/0/0] display this
      #
      interface Serial2/0/0
       link-protocol ppp
      ppp pap local-user huawei password simple huawei
       undo shutdown
      #
      return
      ```

      认证方需要则需要在 AAA 视图下查看用户名及密码。

      ```
      [Huawei] aaa
      [Huawei-aaa] display this
      #
      aaa
       local-user huawei password %$%$04b=C9LzqIsL.w)N+pU<,g^U%$%$
      #
      return
      ```

    - 验证方配置用户名方式的 CHAP 认证场景下用户名和密码的查看方式如下：

      被认证方需要查在接口视图下查看用户名，再根据用户名在 AAA 视图下查看密码。

      ```
      [Huawei-Serial2/0/0] display this
      #
      interface Serial2/0/0
       link-protocol ppp
      ppp chap user huawei
       undo shutdown
      #
      return
      [Huawei-Pos1/0/0] aaa
      [Huawei-aaa] display this
      #
      aaa
       local-user huawei password %$%$04b=C9LzqIsL.w)N+pU<,g^U%$%$
      #
      return
      ```

      验证方需要在 AAA 视图下查看用户名和密码。

      ```
      [Huawei] aaa
      [Huawei-aaa] display this
      #
      aaa
       local-user huawei password %$%$04b=C9LzqIsL.w)N+pU<,g^U%$%$
      ```


版权所有 © 华为技术有限公司

```
#
return
```

- 验证方配置没有用名方式的 CHAP 认证，则用户名和密码的查看方式如下：

  被验证方需要在接口视图下查看用户名和密码：

```
[Huawei-Serial2/0/0] display this
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password simple huawei
 undo shutdown
#
return
```

  验证方需要在 AAA 视图下查看用户名和密码：

```
[Huawei] aaa
[Huawei-aaa] display this
#
aaa
 local-user huawei password %$%$04b=C9LzqIsL.w)N+pU<,g^U%$%$
#
return
```

- 如果都正确，请执行**步骤 2**。

步骤 2 检查接口是否为物理 Up 状态。

执行命令 **display interface** *interface-type interface-number* 查看接口物理状态：

- 如果接口物理状态不是 Up，请处理接口物理故障。详细的故障处理方法请参见物理对接类问题的定位。
- 如果接口状态是 Up，请执行**步骤 3**。

步骤 3 检查接口的协议报文是否收发正常。

执行 **display interface** *interface-type interface-number* 查看接口报文收发个数以确认报文是否收发正常。

```
[Huawei] display interface Serial 2/0/0
Serial2/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-02-05 06:35:43
Description:HUAWEI, AR Series, Serial2/0/0 Interface
Route Port,The Maximum Transmit Unit is 4470, Hold timer is 10(sec)
Internet Address is 108.108.1.1/24
Link layer protocol is PPP
LCP opened, IPCP opened
The Vendor PN is HFBR-57E0P
The Vendor Name is AVAGO
Port BW: 155M, Transceiver max BW: 155M, Transceiver Mode: MultiMode
WaveLength: 1310nm, Transmission Distance: 2000m
Physical layer is Packet Over SDH
Scramble enabled, clock master, CRC-32, loopback: none
Flag J0 "NetEngine       "
Flag J1 "NetEngine       "
Flag C2 22(0x16)
    SDH alarm:
        section layer:  none
        line    layer:  none
        path    layer:  none
    SDH error:
        section layer:  B1 0
        line    layer:  B2 0  REI 44
        path    layer:  B3 0  REI 23
Statistics last cleared:never
    Last 300 seconds input rate 24 bits/sec, 0 packets/sec
```


版权所有 © 华为技术有限公司

```
Last 300 seconds output rate 24 bits/sec, 0 packets/sec
Input: 70945 packets, 1135144 bytes
Input error: 0 shortpacket, 0 longpacket, 0 CRC, 0 lostpacket
Output: 70945 packets, 1135140 bytes
Output error: 0 lostpackets
Output error: 0 overrunpackets, 0 underrunpackets
```

- 如果接收或者发送的报文数量是 0，或者多次显示发现接收或者发送的报文个数没有增长，说明报文在链路上丢失，请先确认物理连接是否正确，请参见物理对接中“物理接口不能 up 定位思路”一节。
- 如果物理连接正确，请处理报文所丢失的故障。
- 如果报文收发正常，请执行步骤 4。

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

此外，还可以打开 **debugging ppp all interface** *interface-type interface-number*，来查看 PPP 协议报文收发以及 PPP 状态机的状态变化情况。

```
Jun  2 2010 17:19:41.310.1 Huawei PPP/7/debug2:Slot=1;
  PPP Event:
      Serial2/0/0 LCP TO+(Timeout with counter > 0)  Event
      state acksent , Retransmit = 4
Jun  2 2010 17:19:41.310.2 Huawei PPP/7/debug2:Slot=1;
  PPP Packet:
      Serial2/0/0 Output LCP(c021) Pkt, Len 18
      State acksent, code ConfReq(01), id 3, len 14
      MRU(1), len 4, val 1176
      MagicNumber(5), len 6, val 00abb891
Jun  2 2010 17:19:41.310.1 Huawei PPP/7/debug2:Slot=1;
  PPP Packet:
      Serial2/0/0 Input  LCP(c021) Pkt, Len 18
      State acksent, code ConfAck(02), id 3, len 14
      MRU(1), len 4, val 1176
      MagicNumber(5), len 6, val 00abb891
Jun  2 2010 17:19:41.310.2 Huawei PPP/7/debug2:Slot=1;
  PPP Event:
      Serial2/0/0 LCP RCA(Receive Config Ack)  Event
      state acksent
```

步骤 4 检查链路是否存在环路。

执行命令 **display interface** *interface-type interface-number* 查看接口物理状态：

```
[Huawei] display interface Serial 2/0/0
Serial2/0/0 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Serial 2/0/0 Interface
Route Port,The Maximum Transmit Unit is 4470, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP, loopback is detected
LCP closed
The Vendor PN is HFBR-57E0P
The Vendor Name is AVAGO
Port BW: 155M, Transceiver max BW: 155M, Transceiver Mode: MultiMode
WaveLength: 1310nm, Transmission Distance: 2000m
Physical layer is Packet Over SDH
Scramble enabled, clock master, CRC-32, loopback: local
Flag J0 "NetEngine       "
```


版权所有 © 华为技术有限公司

```
Flag J1 "NetEngine       "
Flag C2 22(0x16)
    SDH alarm:
        section layer:  none
        line    layer:  none
        path    layer:  none
    SDH error:
        section layer:  B1 22
        line    layer:  B2 94  REI 145
        path    layer:  B3 44  REI 86
Statistics last cleared:never
    Last 300 seconds input rate 56 bits/sec, 0 packets/sec
    Last 300 seconds output rate 56 bits/sec, 0 packets/sec
    Input: 40530 packets, 890400 bytes
    Input error: 0 shortpacket, 0 longpacket, 2 CRC, 0 lostpacket
    Output: 36512 packets, 946612 bytes
    Output error: 0 lostpackets
    Output error: 0 overrunpackets, 0 underrunpackets
```

- 如果有 **loopback is detected**，显示说明链路存在环路，请确认环路产生的原因，并消除环路。
- 如果不存在环路，请执行**步骤 5**。

步骤 5 检查链路延时是否影响上层业务。

在 PPP 协商过程中，华为路由器设备上 PPP 协议报文的超时时间可配。缺省情况下，超时时间是 3 秒，最大可配 PPP 协议报文的超时时间是 10 秒。如果在超时时间内没有收到对端的应答报文，则 PPP 将会重发前一次发送的报文。所以，要保证链路延时小于当前所配置的 PPP 协议报文的超时时间。

请使用测试设备提前检测链路的延时。

- 如果时延已经影响上层业务：
  - 如果链路时延小于 10 秒，执行 **ppp timer negotiate** 命令配置 PPP 协议报文的超时时间小于链路时延。

    配置完成后如果链路时延依旧影响上层业务，请更换相应的设备或者进行相应的维修处理。
  - 如果链路延时大于 9 秒，请更换相应的设备或者进行相应的维修处理。
- 如果时延不影响上层业务，请执行**步骤 6**。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

5.8 xDSL 故障处理

介绍了 xDSL 常见故障的定位思路和案例。

5.8.1 ADSL 接口在 ATM 模式下报文转发不通的定位思路

介绍 ADSL 接口在 ATM 模式下报文转发不通的故障处理流程和详细的故障处理步骤。

说明

ADSL 接口只有 ATM 工作模式。

常见原因

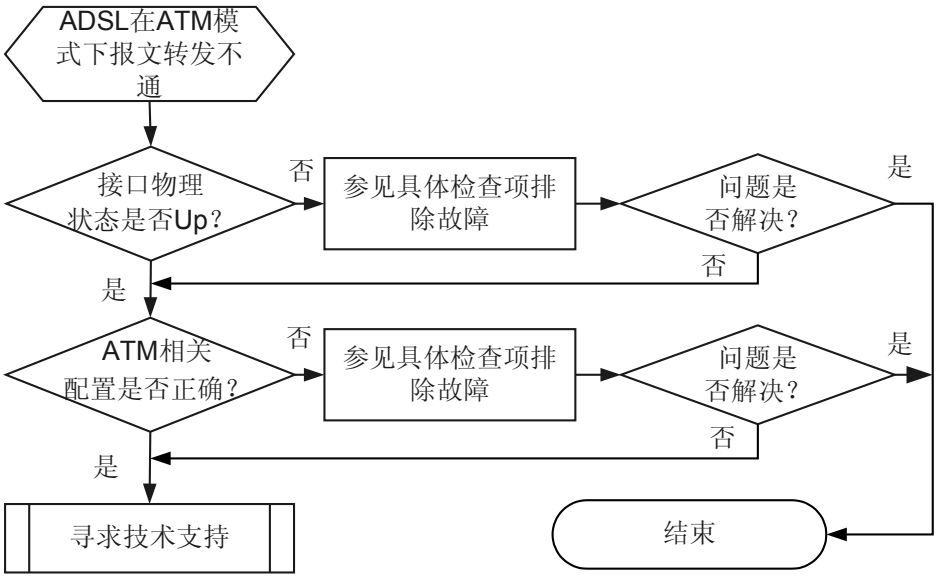
本类故障的常见原因主要包括：

- 接口线缆没有连接好或接口被 **shutdown**。
- 本端和对端 ADSL 接口的传输模式不一致。

故障诊断流程

详细处理流程如图 5-12 所示。

图 5-12 ADSL 在 ATM 模式下报文转发不通的故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查 ADSL 接口物理状态是否 Up。

在系统视图下执行 **display interface atm** 命令查看 ADSL 接口物理状态是否 Up。这里以查看 Atm1/0/0 接口状态为例。

- 如果接口状态显示信息为“Atm1/0/0 current state : Administratively DOWN”，表示接口被 **shutdown**，请先在接口下执行 **undo shutdown** 命令开启接口。执行 **undo shutdown** 命令后如果接口的状态信息为“Atm1/0/0 current state : DOWN”，请参考接口状态显示信息为“Atm1/0/0 current state : DOWN”时的检查项继续检查。
- 如果接口的状态显示信息为“Atm1/0/0 current state : DOWN”，请执行如下检查。

检查项	检查标准	后续操作
检查本端和对端接口缆连接是否正常。	-	正确连接后，故障仍然存在请尝试更换线缆。
检查本端 ADSL 接口的传输标准。	在系统视图下执行 **display dsl interface atm** 命令查看 ADSL 接口配置的上行线路参数，其中“Transmission mode : ”字段对应的显示信息表示 ADSL 接口的传输标准，本端和对端的传输标准必须一致。	如果本端采用的传输标准和对端不一致，请在 ADSL 接口视图下执行 **adsl standard** 命令重新配置接口的传输标准，使两端的传输标准一致。

执行上述操作后如果接口物理状态仍为“DOWN”，请执行步骤 3。

- 如果有“Atm1/0/0 current state : UP”信息证明接口状态为 Up，请执行步骤 2。

步骤 2 检查 ATM 相关配置是否正确。

- 如果配置的是 ATM 链路上承载 IP 报文，请做如下检查。

检查项	检查标准	后续操作
在 ADSL 接口视图下使用 **display this** 命令查看本端 ADSL 接口 IP 地址是否和对端在同一网段。	本端地址需要和对端地址在同一个网段。	如果配置的地址和对端不在同一网段，请在 ADSL 接口视图下使用 **ip address** 命令修改接口 IP 地址。
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 IPoA 映射是否配置正确。	配置的映射地址必须是对端的地址。	如果配置的地址不是对端的地址，请在 ATM-PVC 视图下使用 **map ip** 命令修改配置的映射地址。

- 如果配置的是 ATM 链路上承载 IPoE 报文，请做如下检查。

版权所有 © 华为技术有限公司

检查项	检查标准	后续操作
在 VE 接口视图下使用 **display this** 命令查看本端 VE 接口 IP 地址是否和对端在同一网段。	本端地址需要和对端地址在同一个网段。	如果配置的地址和对端不在同一网段，请在 VE 接口视图下使用 **ip address** 命令修改接口 IP 地址。
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 IPoEoA 映射是否配置正确。	配置的映射 VE 接口和规划中的一致。	如果配置的 VE 接口错误，请在 ATM-PVC 视图下使用 **map bridge** 重新创建 PVC 上的 IPoEoA 映射。

- 如果配置的是 ATM 链路上承载 PPPoA 报文，请做如下检查。

检查项	检查标准	后续操作
检查本端配置的 PPP 认证用户名和密码是否和对端一致。	本端配置的用户名和密码和对端一致。	如果不一致，请在 VT 接口视图下使用 **ppp pap local-user** 或 **ppp chap password** 命令修改 PPP 认证的用户名和密码。
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 PPPoA 映射是否配置正确。	配置的映射 VT 接口和规划中的一致。	如果配置的 VT 接口错误，请在 ATM-PVC 视图下使用 **map ppp** 重新创建 PVC 上的 IPoEoA 映射。

- 如果配置的是 ATM 链路上承载 PPPoEoA 报文，请做如下检查。

检查项	检查标准	后续操作
检查本端拨号口配置的 PPP 认证用户命令和密码是否和对端一致。	本端配置的用户名和密码和对端一致。	如果不一致，请在 VT 接口视图下使用 **ppp pap local-user** 或 **ppp chap password** 命令修改 PPP 认证的用户名和密码。 .
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 PPPoEoA 映射是否配置正确。	配置的映射 VE 接口和规划中的一致。	如果配置的 VE 接口错误，请在 ATM-PVC 视图下使用 **map bridge** 重新创建 PVC 上的 PPPoEoA 映射。

执行完上述检查后故障依然存在请执行步骤 3。

步骤 3 请收集如下信息，并联系华为技术支持工程师。

版权所有 © 华为技术有限公司

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

5.8.2 G.SHDSL 接口在 ATM 模式下报文转发不通的定位思路

介绍 G.SHDSL 接口在 ATM 模式下报文转发不通的故障处理流程和详细的故障处理步骤。

常见原因

本类故障的常见原因主要包括：

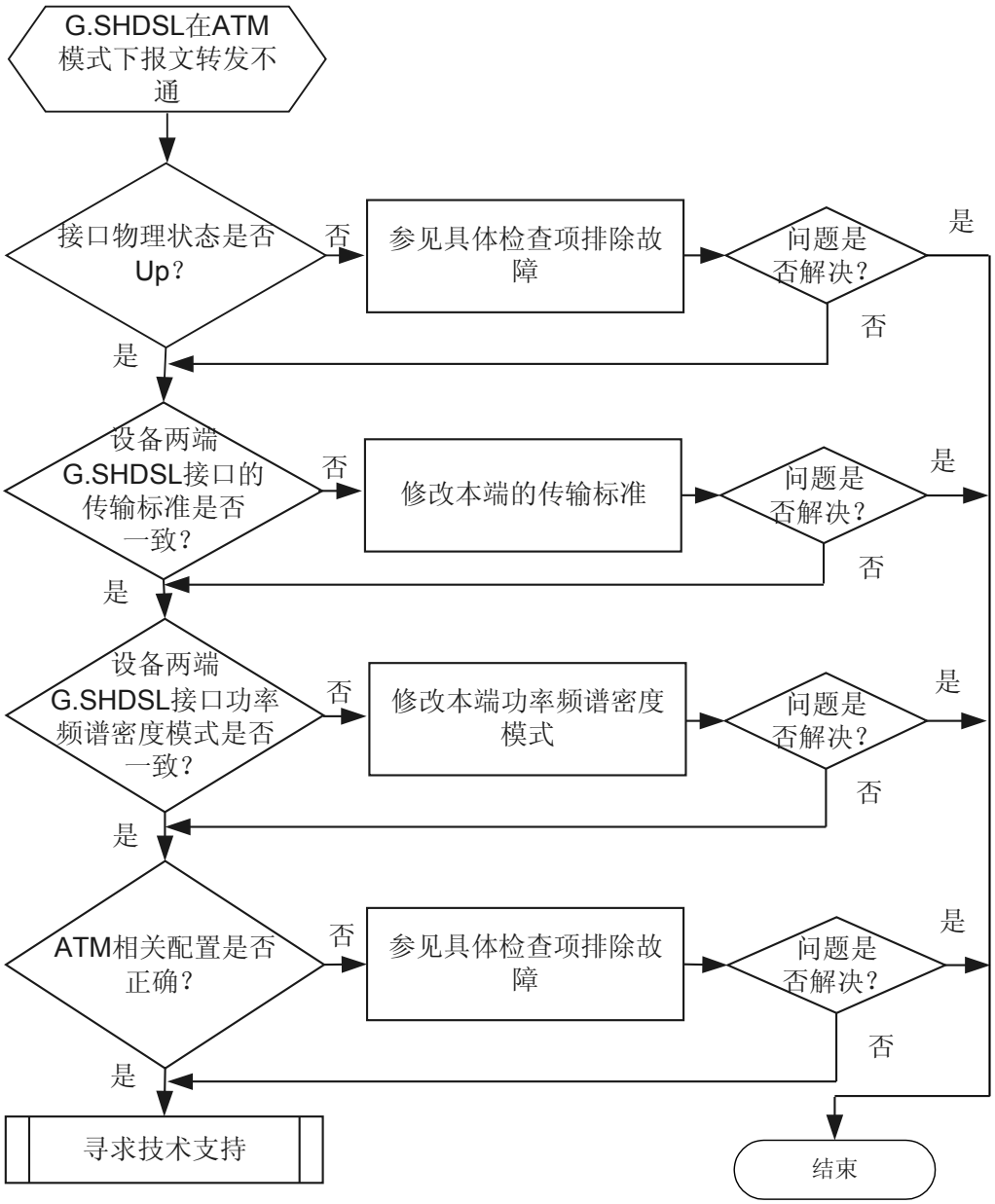
- 接口线缆没有连接好或接口被 **shutdown**。
- 本端和对端 G.SHDSL 接口使用的传输标准不一致。
- 本端和对端功率频谱密度模式不一致。

故障诊断流程

详细处理流程如图 **5-13** 所示。

版权所有 © 华为技术有限公司

图 5-13 G.SHDSL 在 ATM 模式下报文转发不通的故障诊断流程图



故障处理步骤

操作步骤

步骤 1 检查 G.SHDSL 接口物理状态是否 Up。

在系统视图下执行 **display interface atm** 命令查看 G.SHDSL 接口物理状态是否 Up。这里以查看 Atm1/0/0 接口状态为例。

- 如果接口状态显示信息为“Atm1/0/0 current state : Administratively DOWN”，表示接口被 **shutdown**，请先在接口下执行 **undo shutdown** 命令开启接口。执行 **undo**

版权所有 © 华为技术有限公司

shutdown 命令后如果接口的状态信息为“Atm1/0/0 current state : DOWN”，请参考接口状态显示信息为“Atm1/0/0 current state : DOWN”时的检查项继续检查。

- 如果接口状态显示信息为“Atm1/0/0 current state : DOWN”请执行如下检查。

检查项	检查标准	后续操作
检查本端和对端接口缆连接是否正常。	-	正确连接后，故障仍然存在请尝试更换线缆。
在系统视图下执行 **display dsl interface** 命令查看 G.SHDSL 接口绑定模式、主接口和绑定接口的数目。	显示信息中“Port bind status”表示接口的绑定状态，其中： ● Normal ：未绑定。 ● MPair-X：M-Pair 绑定，X 为实际绑定的接口数目。 ● EFM-X：EFM 绑定，X 为实际绑定的接口数目。 显示信息中“ Bind group master port”表示绑定的主接口。 检查标准三要素： ● 设备两端的 G.SHDSL 接口绑定模式必须一致。 ● 设备两端绑定接口的数目必须一致。 ● 设备两端绑定的主接口必须一致。	如果设备两端的 G.SHDSL 接口绑定模式、主接口和绑定接口的数目不一致。 1. 在 G.SHDSL 的 4 个接口下分别执行如下操作： ● 执行 **shutdown** 命令关闭接口。 ● 执行 **undo shdsl bind** 清除接口上当前绑定的配置。 2. 在全局视图下，执行 **set workmode slot** *slot-id* **shdsl** { **atm** | **ptm** }命令修改本端的绑定模式和对端一致。 3. 根据对端的主接口确定本端的主接口，在本端主接口下执行 **shdsl bind** 命令修改本端绑定接口的数目和对端一致。

执行上述操作后如果接口状态显示信息仍为“Atm1/0/0 current state : DOWN”，请执行步骤 5。

- 如果有“Atm1/0/0 current state : UP”信息证明接口状态为 Up，请执行步骤 2。

步骤 2 检查本端和对端 G.SHDSL 接口使用的传输标准是否一致。

在系统视图下执行 **display dsl interface** 命令查看 G.SHDSL 接口配置的传输标准。其中显示信息中“Port transmission mode : ”字段对应的内容表示当前接口采用的传输标准。

- 如果本端采用的传输标准和对端不一致，请在 G.SHDSL 接口视图下执行 **shdsl annex** 命令重新配置接口的传输标准，使两端的传输模式一致。
- 如果本端采用的传输标准和对端一致，请执行步骤 3。

步骤 3 检查本端和对端 G.SHDSL 接口的功率频谱密度模式是否一致。

在系统视图下执行 **display dsl interface** 命令查看 G.SHDSL 接口配置的功率频谱密度模式。其中显示信息中“Port power spectral density : ”字段对应的内容表示当前接口采用的功率频谱密度模式。

- 如果本端采用的功率频谱密度模式和对端不一致，请在 G.SHDSL 接口视图下执行 **shdsl psd** 命令重新配置接口的功率频谱密度模式，使两端保持一致。

版权所有 © 华为技术有限公司

- 如果本端采用的功率频谱密度模式和对端一致，请执行步骤 4。

步骤 4 检查 ATM 相关配置是否正确。

- 如果配置的是 ATM 链路上承载 IP 报文，请做如下检查。

检查项	检查标准	后续操作
在 G.SHDSL 接口视图下使用 **display this** 命令查看本端 G.SHDSL 接口 IP 地址是否和对端在同一网段。	本端地址需要和对端地址在同一个网段。	如果配置的地址和对端不在同一网段，请在 G.SHDSL 接口视图下使用 **ip address** 命令修改接口 IP 地址。
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 IPoA 映射是否配置正确。	配置的映射地址必须是对端的地址。	如果配置的地址不是对端的地址，请在 ATM-PVC 视图下使用 **map ip** 命令修改配置的映射地址。

- 如果配置的是 ATM 链路上承载 IPoE 报文，请做如下检查。

检查项	检查标准	后续操作
在 VE 接口视图下使用 **display this** 命令查看本端 VE 接口 IP 地址是否和对端在同一网段。	本端地址需要和对端地址在同一个网段。	如果配置的地址和对端不在同一网段，请在 VE 接口视图下使用 **ip address** 命令修改接口 IP 地址。
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 IPoEoA 映射是否配置正确。	配置的映射 VE 接口和规划中的一致。	如果配置的 VE 接口错误，请在 ATM-PVC 视图下使用 **map bridge** 重新创建 PVC 上的 IPoEoA 映射。

- 如果配置的是 ATM 链路上承载 PPPoA 报文，请做如下检查。

检查项	检查标准	后续操作
检查本端配置的 PPP 认证用户名和密码是否和对端一致。	本端配置的用户名和密码和对端一致。	如果不一致，请在 VT 接口视图下使用 **ppp pap local-user** 或 **ppp chap password** 命令修改 PPP 认证的用户名和密码。

版权所有 © 华为技术有限公司

检查项	检查标准	后续操作
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 PPPoA 映射是否配置正确。	配置的映射 VT 接口和规划中的一致。	如果配置的 VT 接口错误，请在 ATM-PVC 视图下使用 **map ppp** 重新创建 PVC 上的 IPoEoA 映射。

- 如果配置的是 ATM 链路上承载 PPPoEoA 报文，请做如下检查。

检查项	检查标准	后续操作
检查本端拨号口配置的 PPP 认证用户命令和密码是否和对端一致。	本端配置的用户名和密码和对端一致。	如果不一致，请在 VT 接口视图下使用 **ppp pap local-user** 或 **ppp chap password** 命令修改 PPP 认证的用户名和密码。
在 ATM-PVC 视图下使用 **display this** 命令查看 PVC 上的 PPPoEoA 映射是否配置正确。	配置的映射 VE 接口和规划中的一致。	如果配置的 VE 接口错误，请在 ATM-PVC 视图下使用 **map bridge** 重新创建 PVC 上的 PPPoEoA 映射。

执行完上述检查后故障依然存在请执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

5.9 3G 故障处理

5.9.1 拨号参数配置 OK，3G 呼叫失败的定位思路

版权所有 © 华为技术有限公司

常见原因

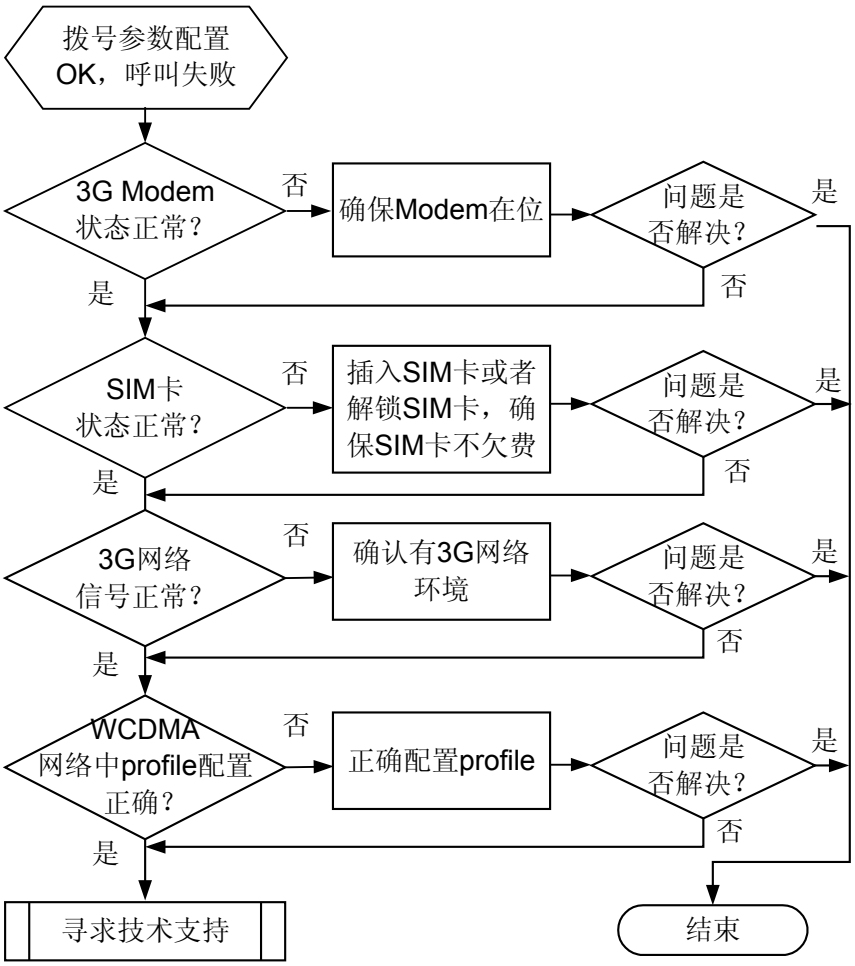
本类故障的常见原因主要包括：

- 3G Modem 状态不正常，如 Modem 没有插好
- SIM 卡状态不正常，如 SIM 卡没有插好、SIM 卡需要 PUK 解锁、SIM 卡欠费
- 3G 信号未覆盖 AR 上的 3G 数据卡
- 使用 WCDMA 网络，Modem 的 profile 未配置正确

故障诊断流程

详细处理流程如图 5-14 所示。

图 5-14 3G 呼叫失败的故障诊断流程图



故障处理步骤

版权所有 © 华为技术有限公司

说明

AR 支持 WCDMA 和 CDMA2000，不支持 TD-SCDMA。

请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。

操作步骤

步骤 1 执行 **display interface cellular** *interface-number* 命令，查看 **USB Modem State** 字段。

```
<Huawei> display interface cellular 0/0/0
Cellular0/0/0 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Cellular0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is negotiated, 192.168.70.94/32
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time   : 2011-06-08 10:53:15
Last physical down time : 2011-06-08 10:53:13
Current system time: 2011-06-08 11:35:23
USB Modem State: Present
Last 300 seconds input rate 555 bytes/sec, 4440 bits/sec
Last 300 seconds output rate 0 bytes/sec, 0 bits/sec
    Input: 87205 bytes
    Output:6760917 bytes
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

- 如果为 Not present，表示 3G Modem 不在位。需重新插拔 3G Modem。
- 如果为 Present 是正常的，请执行步骤 2。

步骤 2 执行 **display cellular** *interface-number* **all** 命令，查看 **Network Information** 信息。

如果显示如下内容，则表示当前网络为可用状态。请执行步骤 3。

```
Network Information.
====================
Current Service Status = Service available
Current Service = Combined
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
......
```

如果是其他状态，如 Current Service Status 为 No service 或 Emergency，或者 Packet Service 为 Detached，请执行以下操作：

- 在接口视图下执行 **plmn auto** 命令配置自动方式选择 PLMN。
- 如果是 WCDMA 网络，在接口视图下执行 **mode wcdma wcdma-precedence** 命令将网络连接方式设置为优选 WCDMA。
- 如果是 CDMA2000 网络，在接口视图下执行 **mode cdma hybrid** 命令将将网络连接方式设置为选择 EVDO 和 1x RTT 混合网络。

步骤 3 检查 SIM 卡状态是否正常。

1. 联系网络运营商，确认 SIM 卡已开通 3G 上网服务，且不欠费。
2. 执行 **display cellular** *interface-number* **all** 命令，查看 SIM 卡状态。

版权所有 © 华为技术有限公司

显示信息	处理方法
如果显示以下信息，表明 SIM 卡状态正常。 PIN Verification = Disabled PIN Status = **Ready** Number of Retries remaining = 3 SIM Status = **OK**	请执行步骤 4。
如果显示以下信息，表明设备需要输入 PIN 码解锁。 PIN Verification = Unknown PIN Status = **PIN Requirement** Number of Retries remaining = 3 SIM Status = Invalid	在接口视图下执行 **pin verify** *pin* 命令解锁。 **说明** 如果输入的 PIN 码连续 3 次错误，PIN 码就被锁定，此时需要用 PUK 解锁。
如果显示以下信息，表明设备需要输入 PUK 码解锁。 PIN Verification = Unknown PIN Status = **PUK Requirement** Number of Retries remaining = 10 SIM Status = Invalid	在接口视图下执行 **pin unlock***puk pin* 命令解锁。
如果显示以下信息，表明设备没有插入 SIM 卡。 PIN Verification = Unknown PIN Status = Unknown SIM Status = **Not insert**	请拔下数据卡，插入 SIM 卡之后再插上数据卡。 **说明** SIM 卡不支持热插拔。

执行上述处理后，数据卡会重新开始初始化，请等待 1 分钟左右，尝试重新拨号。如果还是不能成功，请执行步骤 4。

说明

拨号有两种方式:

- 流量触发：就是通过数据流量触发。如点击网页，当数据流量到了 3G 接口，就会触发 3G 接口进行拨号。
- 自动拨号：在接口视图下执行命令 **dialer number *99# autodial**（WCDMA）或 **dialer number #777 autodial**（CDMA2000），系统会定时尝试接入 3G 网络。

步骤 4 检查 3G 网络信号是否正常。

使用其他 3G 设备，如 3G 手机，查看所处环境是否有 3G 信号。

- 如果所处环境没有 3G 信号覆盖，请排除无线接入网络侧的问题。
- 如果 3G 手机可以正常使用，表明网络信号正常，请执行步骤 5。

步骤 5 如果使用 WCDMA 网络，检查 3G Modem 的 profile 配置是否正确。

执行 **display cellular** *interface-number* **all** 命令，查看 **Profile Information** 字段。若显示如下信息，表明没有配置 profile，需要配置 profile。

```
Profile Information.
====================
Profile 1 = UNDEFINED
--------
* - Default profile
```

在接口视图下执行 **profile create 1 static** *apn-name* 命令创建 profile。需要从网络运营商处获得 APN。

版权所有 © 华为技术有限公司

步骤 6 如果故障仍然存在，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

故障处理步骤补充（华为工程师专用）

说明

本节是对“故障处理步骤”的补充。如果华为工程师在执行“故障处理步骤”的步骤后仍不能解决故障，可以根据本节提供的内部定位方法继续定位。

操作步骤

步骤 1 打开 DCC 调试开关，尝试拨号，收集调试信息并联系华为研发工程师。

说明

调试信息在终端显示，先执行 **terminal monitor** 和 **terminal debugging** 命令打开通道。调试结束后，要及时执行 **undo debugging all** 命令关闭调试开关。

命令	功能
debugging dialer all debugging dialer info	打开拨号事件、信息调试开关。
debugging ppp lcp all	打开 PPP 的 lcp 调试开关。
debugging ppp ipcp all	打开 PPP 的 ipcp 调试开关。

----结束

相关告警与日志

相关告警

无

相关日志

- Jun 5 2011 10:0 8:58+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[1]:InFile: ppp_func.c, Line: 1291. Callterface Cellular0/0/0 has turned into UP state.
- Jun 5 2011 10:08:58+00:00 Huawei %%01IFNET/4/LINK_STAT32a771c (PPP_CopyConfigToBChannelE(l)[2]):The line protocol on the interface Cellular0/0/0 has entered the UP state.
- Jun 5 2011 10:08:558(DCC_TaskEntry) <-- 0x004c5f358+00:00 Huawei IFNET/6/ IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Interfa 0x04db8f74(vxTaskEntry) <-- 0x0ce 13 turned into UP state.(AdminStatus 1,OperStatus 1,InterfacepuID: -1, TaskID: 166, Sn: 256> Name Cellular0/0/0)

版权所有 © 华为技术有限公司

- Jun 5 2011 10:08:59+00:00 Huawei %%01IFNET/4/LINK_STATE(l)[3]:The line protocol PPP IPCP on the interface Cellular0/0/0 has entered the UP state.
- Jun 5 2011 10:08:58+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[1]:InFile: ppp_func.c, Line: 1291. Callterface Cellular0/0/0 has turned into DOWN state.
- Jun 5 2011 10:08:58+00:00 Huawei %%01IFNET/4/LINK_STAT32a771c (PPP_CopyConfigToBChannelE(l)[2]):The line protocol on the interface Cellular0/0/0 has entered the DOWN state.
- Jun 5 2011 10:08:558(DCC_TaskEntry) <-- 0x004c5f358+00:00 Huawei IFNET/6/ IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Interfa 0x04db8f74(vxTaskEntry) <-- 0x0ce 13 turned into DOWN state.(AdminStatus 1,OperStatus 1,InterfacepuID: -1, TaskID: 166, Sn: 256> Name Cellular0/0/0)
- Jun 5 2011 10:08:59+00:00 Huawei %%01IFNET/4/LINK_STATE(l)[3]:The line protocol PPP IPCP on the interface Cellular0/0/0 has entered the DOWN state.

版权所有 © 华为技术有限公司

6 语音类

关于本章

6.1 语音故障处理

版权所有 © 华为技术有限公司

6.1 语音故障处理

6.1.1 摘机后无拨号音的定位思路

常见原因

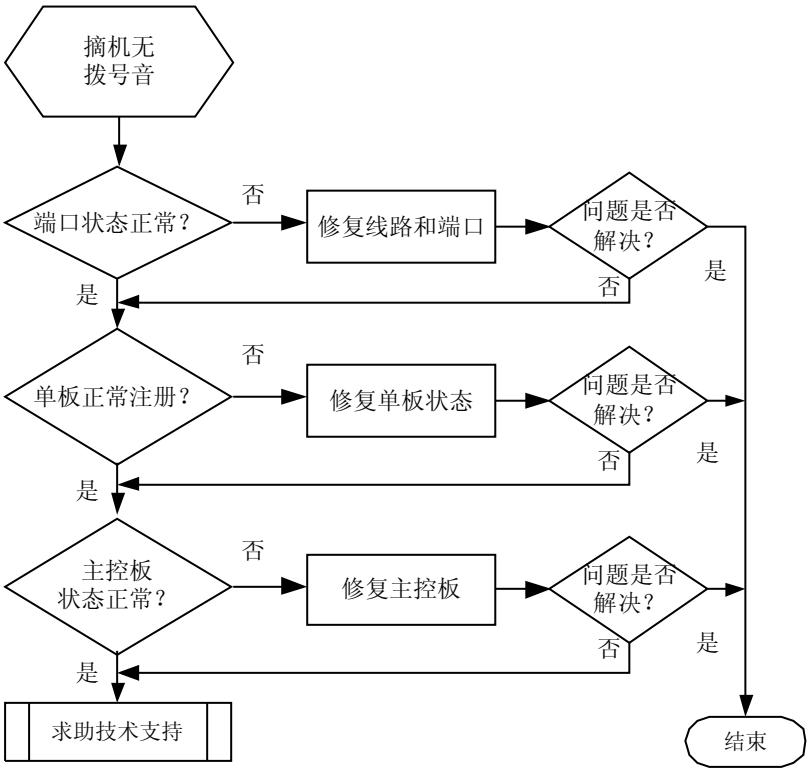
此类故障的种常见原因包括：

- 外线和端口数据原因
- 接口板是否正常注册
- 系统内部问题

故障诊断流程

详细故障处理流程，如图 6-1 所示。

图 6-1 摘机无拨号音故障定位思路



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查摘机后端口状态

使用 **display voice port fxs state** *slotid/subcardid/portid* 命令，在接入设备侧检查用户摘机后端口状态是否变成 **in service** 状态，以判断用户线路连接正确

```
[Huawei-voice] display voice port fxs state 1/0/0
 port FXS state: 1/0/0
 PTPSrvState      : Normal
 PTPAdmState      : NoLoop,NoTest
 CTPSrvState      : In serivce
 CTPAdmState      : StartSvc
 LineState        : Normal
```

- 如果端口状态不正常，请修复用户线路。
- 如果端口状态正确，请执行步骤 2。

步骤 2 检查单板是否正常注册

如果单板没有正常注册，摘机后高层协议不能正常交互，也会导致不放拨号音。使用 **display device** 命令查看单板状态,“Registered”表示单板注册成功，“Unregistered”表示未注册。

- 如果单板状态不正常，请尝试修复单板。
- 如果单板状态正常，则执行步骤 3。

步骤 3 检查主控板状态

以上步骤 1、2 排查无误，可能是主控板或者系统语音文件问题。可以尝试进行主控板测试。

- 如果主控板状态不正常，请修复主控板。
- 如果主控板状态正常，则执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

6.1.2 通话质量低的定位思路

常见原因

版权所有 © 华为技术有限公司

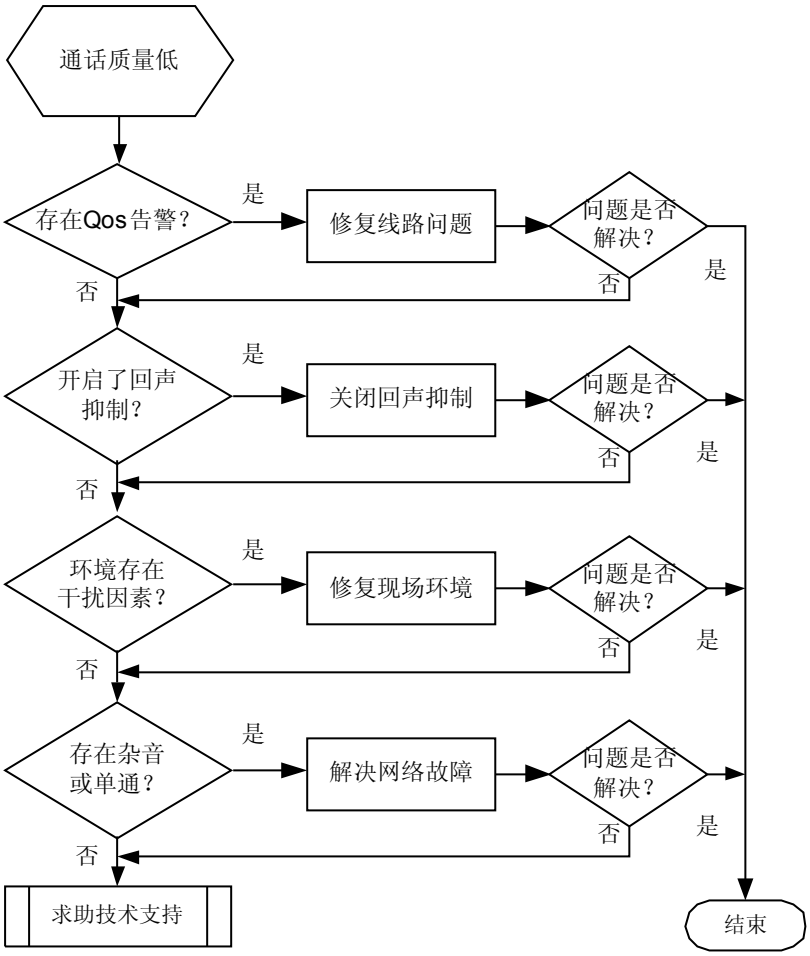
此类故障的种常见原因包括：

- 单通类原因（如，网络存在防火墙类设备屏蔽了 RTP 媒体流端口号）
- 杂音类问题
  - 设备接地不好
  - 周边环境干扰
  - 网络原因
  - 设备硬件原因
- 回音类问题

故障诊断流程

详细故障处理流程，如图 6-2 所示。

图 6-2 通话质量低故障定位思路



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查 Qos 告警记录

检查 AR 设备的历史告警信息，检查是否存在 QoS 告警记录。如果存在 QoS 告警记录，检查告警中相应的对端 IP 记录，排查网络原因。

- 如果有 Qos 告警记录，请修复网络故障。
- 如果无 Qos 告警记录，请执行步骤 2。

步骤 2 检查软交换设备是否开启回声抑制功能

- 如果开启了回声抑制，请尝试关闭此功能。
- 如果未开启回声抑制，则执行步骤 3。

步骤 3 检查现场环境

检查现场环境方面因素，检查是否存在无线基站干扰、广播天线干扰、用户线缆是否与电源线搭接等情况。

- 如果有环境干扰，请尝试排除干扰。
- 如果无环境干扰，则执行步骤 4。

步骤 4 检查杂音、单通等情况

使用软件抓包，听取 wav 文件判断杂音、单通的故障发生点。例如在本地 AR A 和远端 AR B 分别抓包，如果在 A 点转换生成的 wav 文件没有杂音或者单通的现象、而 B 点生成的 wav 文件能够听到杂音或者单通的现象，那么可以确认故障发生在中间的承载网络。

- 如果有杂音、单通等网络问题，请解决网络问题。
- 如果无此类网络问题，则执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

6.1.3 呼叫失败的定位思路

常见原因

版权所有 © 华为技术有限公司

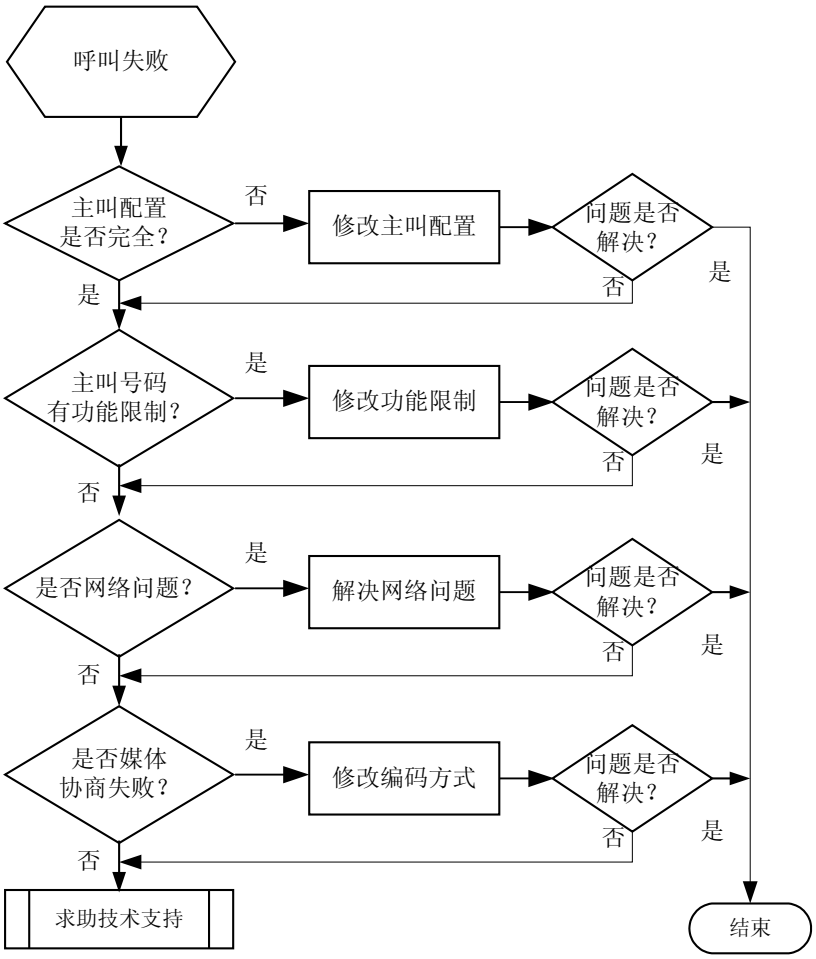
呼叫失败故障包括以下几种常见原因：

- 数图精准性问题
- 网络问题
- 媒体协商问题

故障诊断流程

详细故障处理流程，如图 6-3 所示。

图 6-3 呼叫失败故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查主叫配置是否完全

执行命令 **display voice sipaguser** 查看对应用户的配置，看是否配置完全。如果没有配置则无法发起呼叫。

版权所有 © 华为技术有限公司

- 如果主叫配置不完全，请重新配置。
- 如果主叫配置完整，请执行步骤 2。

步骤 2 检查在软交换侧是否对出现问题的主叫号码进行了功能限制，例如没有开启长权等

可以通过软件在设备上抓取信令，看是否出现发送了 INVITE 以后没有收到 100 Trying 或 180Ringing 之类的信令，而是直接收到了 4XX 或 5XX 之类的消息。

- 如果抓取到相关信令，则先看软交换侧是否已经对主叫号码进行了正确的配置。
- 如果未抓取到相关信令，则执行步骤 3。

步骤 3 检查是否网络问题

在 AR 侧和被叫侧分别跟踪 SIP 信令消息，对信令进行分析，检查确认信令的交互是否正常，可以通过软件抓取信令，如果发现始终只有一个方向的 sip 信令，则可能是网络不通造成的。

如果能够 ping 通但信令不通，请检查 sipag 的配置的 ip 地址端口号等信息是否和信令中的 ip 地址端口号一致，采用如下方法查看 sipag 的信息。

```
<Huawei> display voice sipag 1 config
  AGID                                : 1
  Dynamic signalling IP address name  :
  Signalling IP                       : 192.168.1.1
  Signalling port                     : 5060
  Dynamic media IP address name       :
  Media IP                            : 192.168.1.1
  Transfer mode                       : UDP
  Primary proxy IP 1                  : 2.2.2.2
  Primary proxy IP 2                  : 255.255.255.255
  Secondary proxy IP 1                : 255.255.255.255
  Secondary proxy IP 2                : 255.255.255.255
  Primary proxy port                  : 5060
  Secondary proxy port                : 65535
  Primary proxy domain name           :
  Secondary proxy domain name         :
  Proxy address mode                  : IP
  Home domain name                    : huawei.com
  SIP profile index                   : 1: Default
  Service logic index                 : 0: Default
  Server Address DHCP option          : 0: None
  Description                         :
  AG domain name                      :
  Phone context                       :
  Register URI                        :
  Conference factory URI              :
  Subscribe to UA profile             : Enable
  Subscribe to reg state              : Disable
  Subscribe to MWI                    : Disable
  SDP negotiation mode                : Remote
  Mode of supporting proxy dual-homing : Manual switch over
  Proxy detection mode                : Probe
  Proxy refresh mode                  :
```

- 如果网络存在问题，请解决网络问题。
- 如果网络正常，则执行步骤 4。

步骤 4 检查是否媒体协商问题

对信令进行分析，检查确认媒体协商是否成功。如果媒体协商不成功，则需要被叫侧修改默认的编解码，或调整 AR 设备优选的编解码方式。

使用软件抓取信令，然后看 sdp 协商是否成功。主要关注 invite 和 200 OK 中携带的 SDP 信息。只有两边一致的时候才说明协商成功。

版权所有 © 华为技术有限公司

- 如果媒体协商存在问题，请修改被叫侧缺省的编解码方式。
- 如果媒体协商不存在问题，则执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

6.1.4 SIP 接口故障的定位思路

常见原因

此类故障的种常见原因包括：

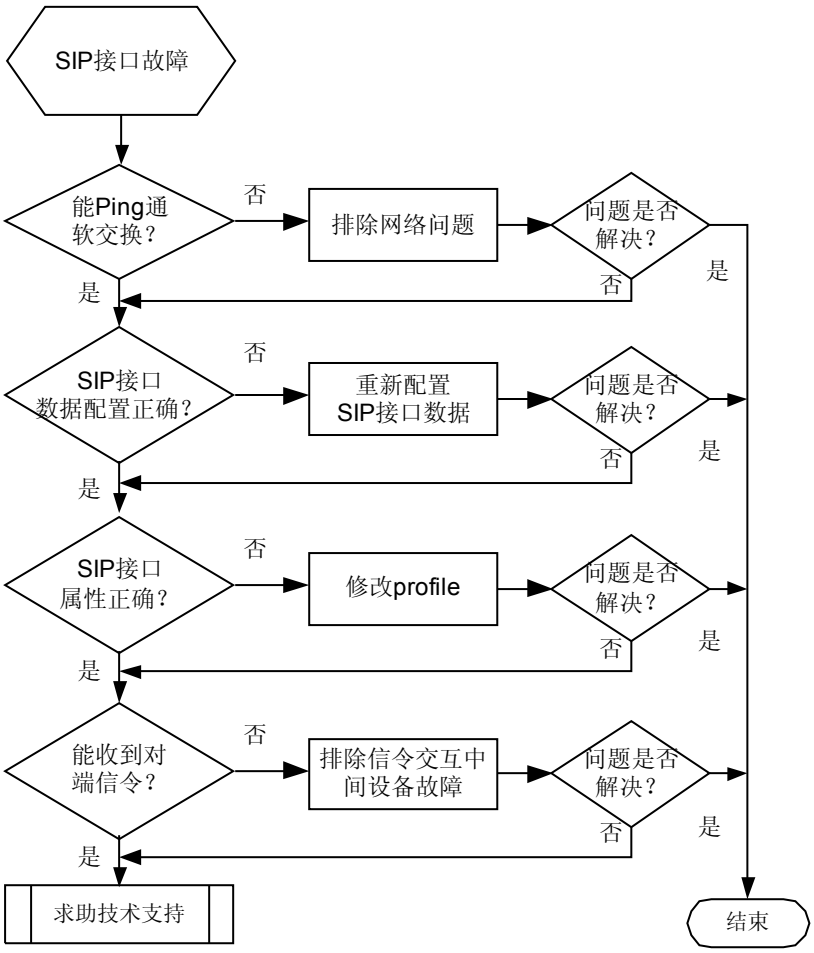
- SIP 接口数据配置错误
- AR 与上级软交换之间的路由
- AR 与其他软交换协议配合类问题
- 回声或其他原因导致信号质量差

故障诊断流程

详细故障处理流程，如图 6-4 所示。

版权所有 © 华为技术有限公司

图 6-4 SIP 接口故障定位思路



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查能否 Ping 通软交换

先执行命令 **display voice sipag** 查看 SIP 接口是否 UP。

然后 Ping 软交换，看看能否 Ping 通。

```
<Huawei> ping 172.183.20.13
```

- 如果 Ping 不通，请检查并解决网络问题。
- 如果能够 Ping 通，执行步骤 2。

步骤 2 检查 SIP 接口的数据是否与上级软交换设备一致

执行命令 **display voice sipag** [*sipag-interface-id* { **running** | **config** }]检查 SIP 接口的配置数据，看是否和软交换的一致。主要关注传输方式，服务器 IP 和服务器的端口号。

- 如果配置存在问题，则重新进行配置。

版权所有 © 华为技术有限公司

- 如果配置正确，则执行步骤 3。

步骤 3 根据上级软交换设备类型，执行命令 **display voice sipag** [*sipag-interface-id* { **running** | **config** }]检查 AR 侧 SIP 接口属性中是否采用了相应的 profile 文件；默认请使用 Default。

- 如果 profile 类型有问题，请使用命令 **profile** 重新配置。
- 如果 profile 类型没有问题，则执行步骤 4。

步骤 4 检查对端信令交互

使用软件对信令进行抓包，分析信令是否在交互路径上的某个设备被丢弃。

- 如果分析出信令在哪个设备上被丢弃，则检查该设备的故障原因。
- 如果无法分析出信令在哪个环节被丢弃，则执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

7 IP 转发及路由类

关于本章

7.1 Ping 故障处理
介绍 Ping 不通故障的定位思路和典型案例。

7.2 DHCP 故障处理
介绍 DHCP 常见故障的定位思路。

7.3 RIP 故障处理

7.4 OSPF 故障处理

华为专有和保密信息
版权所有 © 华为技术有限公司

7.1 Ping 故障处理

介绍 Ping 不通故障的定位思路和典型案例。

7.1.1 Ping 不通问题的定位思路

常见原因

Ping 不通指的是在源端发送请求报文后，在一定的时间范围内没有收到目的端对该请求的回应。

本类故障的常见原因主要包括：

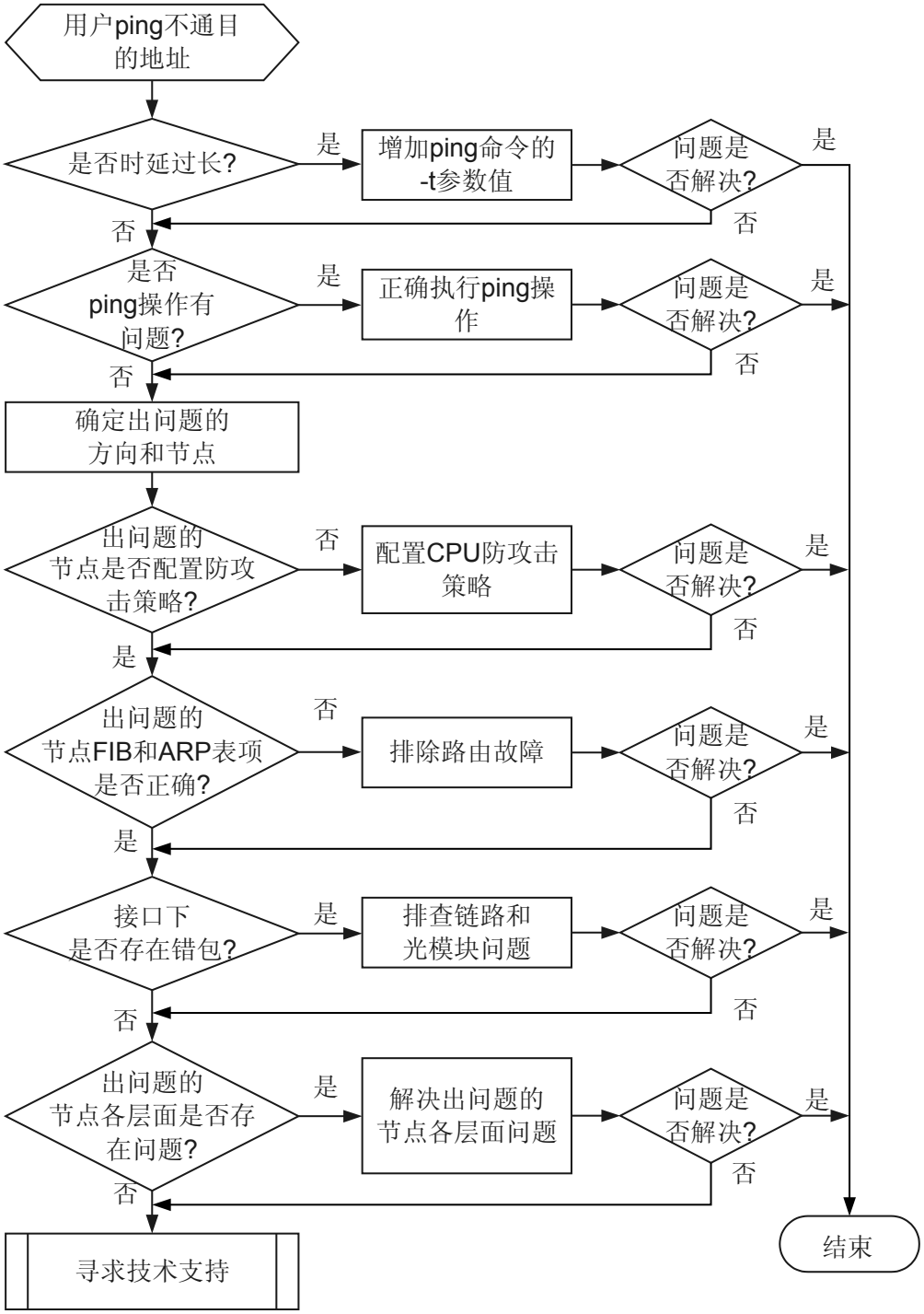
- 链路传输时延较长。由于传输时延长，虽然源端接收到了目的端的回应报文，但已经超过等待时限而造成的 PING 不通的现象。
- 操作不当。例如当 Ping 报文过大时，报文的出接口 MTU 值较小，但是又设置了不可分片的功能等。
- 路由表项或 ARP 表项（ARP 表项只针对以太链路）有问题。
- 硬件故障。

故障诊断流程

可按照故障诊断流程图 7-1 排除此类故障。

版权所有 © 华为技术有限公司

图 7-1 IP 转发不通故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查是否链路传输时延较长导致 Ping 不通

执行 **ping -t** *time-value* **-v** *destination-address* 命令确认是否链路传输时延较长导致 Ping 不通。

说明

-t 参数用来设置等待目的端响应报文的超时时间，默认为 2000ms；**-v** 参数用来显示接收到的非期望回应报文，缺省是不显示。

Ping 的原理是在特定时间内收到回应报文就表示能 Ping 通，否则就表示 Ping 不通。因此首先通过设置 Ping 的**-t** 和**-v** 参数排除由于传输时延较长造成的 Ping 不通。如果是传输时延较长导致的丢包会打印如下信息：

```
<Huawei> ping -v -t 1 10.1.1.1
     PING 10.1.1.1: 56  data bytes, press CTRL_C to break
       Request time out
Error:  Sequence number = 1 is less than the correct = 2!
```

出现如上提示信息则说明是链路传输时延较长造成的 Ping 不通，请增大**-t** 参数的值。

如果**-t** 值较大时才能 Ping 通，请检查设备的状态和链路情况，排除网络和设备异常导致的 Ping 不通情况。

如果增大**-t** 参数的值，仍 Ping 不通，请执行步骤 2。

说明

如果在 PE 端 Ping 私网地址，需使用命令 **ping -vpn-instance** *vpn-name destination-address*，其中的**-vpn-instance** *vpn-name* 指 Ping 的目的地址所属的 VPN 实例。

步骤 2 检查是否操作错误

1. 检查是否执行了 **ping -f**，如果执行此操作，则该 Ping 报文不支持分片，此时需要检查路径上出接口的 MTU 值是否小于 Ping 的报文大小，如果 MTU 小于 Ping 报文大小，则丢失为正常现象，请更改 Ping 报文大小小于 MTU 值，否则请执行子步骤 b。查看接口的 MTU 值可执行如下命令：

   ```
   <Huawei> display interface gigabitethernet 1/0/0
   GigabitEthernet1/0/0 current state : UP
   Line protocol current state : UP
   Description:HUAWEI, AR Series, GigabitEthernet1/0/0 Interface
   Route Port,The Maximum Transmit Unit is 1500
   ```

2. 请检查是否是执行了 **ping -i**，即指定出接口。如果指定的出接口是以太链路等广播类型接口，只支持 Ping 的目的地址是直连接口地址的情况。如果不满足此条件，请更改 Ping 的操作。如果操作无误后故障仍然存在，请执行步骤 3。

说明

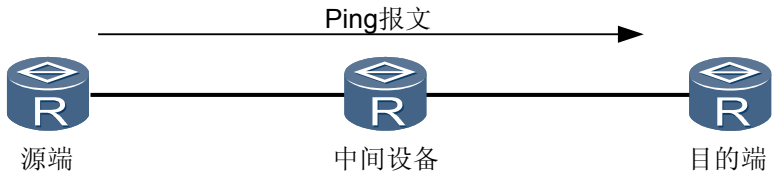
f 参数用来设置该 Ping 报文不支持分片。**-i** *interface-name* 参数用来指定 Ping 报文的出接口，此时会把目的 IP 地址作为下一条地址进行处理。

步骤 3 确定出问题的方向

Ping 应用场景包含三个角色：Ping 报文发起端（源端），中间设备和 Ping 报文接收端（目的端）。故障可能发生在其中任何一个设备的发送或接收方向，因此要确定出故障的方向和节点，缩小定位范围。

版权所有 © 华为技术有限公司

图 7-2 Ping 应用场景



确定报文是在从源端至目的端的路径出现问题，还是在反方向出现问题。在源端和目的端停止 Ping 操作，通过 **display icmp statistics** 查看 ICMP 报文收发情况，如下：

```
<Huawei> display icmp statistics
  Input: bad formats            0     bad checksum                  0
         echo                  36     destination unreachable       9
         source quench          0     redirects                    43
         echo reply            18     parameter problem             0
         timestamp              0     information request           0
         mask requests          0     mask replies                  0
         time exceeded          6
         Mping request          0     Mping reply                   0
  Output:echo                  20     destination unreachable   71438
         source quench          0     redirects                     0
         echo reply            36     parameter problem             0
         timestamp              0     information reply             0
         mask requests          0     mask replies                  0
         time exceeded          0
         Mping request          0     Mping reply                   0
```

说明

在发送端，使用命令 **display icmp statistics** 命令查看主控板的报文统计信息。

在接收端，使用命令 **display icmp statistics** 命令查看对应接口板的报文统计信息。

- 如果 ICMP 报文计数没有增长，则单板或设备上没有其他上送的 ICMP 报文（比如网管的报文）。请执行如下步骤：

  执行 **ping** 操作，再次使用 **display icmp statistics** 命令查看 ICMP 报文收发情况。

  根据统计信息中 Input/Output 包的数量可以确定 Ping 出现问题的方向，如下：

  - 源端 Output:echo 值正常增加，Input:echo 没有增加；目的端 Input/Output 都没有变化。说明源端发出了请求但是没有收到回应，而在目的端没有收到请求，因此可以确定 Ping 在源端->目的端方向出现问题。
  - 源端 Output:echo 值正常增加，Input:echo 没有增加；目的端 Input/Output:echo 都正常增加。说明源端发出了请求但是没有收到回应，而在目的端收到请求，同时发出了回应，因此可以确定 Ping 包在目的端->源端方向出现问题。

  确定了出问题的方向后，请执行步骤 4。

- 如果 ICMP 报文计数仍在增长，则单板或是设备上有其他上送的 ICMP 报文。请执行如下步骤：

  说明

  此方法需要在以下前提下进行:

  - 确保不影响现网业务。
  - 相应接口下相应方向没有应用流量策略。

  1. 依次在每台设备上配置 ACL，通过源和目的 IP 地址匹配 Ping 报文。

     配置文件如下：

     ```
     statistics enable
     #
     ```


版权所有 © 华为技术有限公司

```
acl number 3000
rule 5 permit ip source 1.1.1.1 0 destination 1.1.1.2 0
#
traffic classifier 3000 operator or
if-match acl 3000
#
traffic behavior 3000
#
traffic policy 3000
statistics enable
classifier 3000 behavior 3000
```

2. 在接口视图下使用命令 **traffic-policy**，依次在接口上应用 ACL。
   - 对于 Ping 的发起端和接收端：在接口的 inbound 方向应用该流量策略。
   - 对于中间设备：在接口的 inbound 和 outbound 方向都应用该流量策略。

   配置文件举例如下：

```
#
interface gigabitethernet 1/0/0
 ip address 1.1.1.2 255.255.255.252
 traffic-policy 3000 inbound
#
interface gigabitethernet 2/0/0
 traffic-policy 3001 outbound
#
display traffic policy statistics interface
```

   说明

   当应用流量策略的接口是 Trunk 或 VLANIF 时，流量策略需要配置在成员物理接口下。

3. 使用命令 **display traffic policy statisticsinterface**，依次在每台设备的接口上查看 ACL 的命中情况。

```
<Huawei> display traffic policy statistics interface gigabitethernet 1/0/0 inbound
Interface: GigabitEthernet1/0/0
inbound: test
Traffic policy applied at 2007-08-30 18:30:20
Traffic policy Statistics enabled at 2007-08-30 18:30:20
Statistics last cleared: Never
Rule number: 7 IPv4, 1 IPv6
Current status: OK!
Item                              Packets                    Bytes
-------------------------------------------------------------------
Matched                             1,000                  100,000
  +--Passed                           500                   50,000
  +--Dropped                          500                   50,000
    +--Filter                         100                   10,000
    +--URPF                           100                   10,000
    +--CAR                            300                   30,000
Missed                              500                   50,000
Last 30 seconds rate
```

   - 如果 ACL 完全命中，则说明 Ping 报文发送或接收正常。如果仍无法 Ping 通，请保留上述信息，联系华为技术工程师。
   - 如果中间设备的 inbound 和 outbound 方向的 ACL 完全命中，则说明中间设备正常。需要排查发起端或目的端问题。
   - 如果某设备的 inbound 方向没有命中，则为 Ping 报文相应方向的上游设备故障。请在故障设备上执行步骤 5。

步骤 4 确定出问题的节点

从出问题方向顺序定位。

- 源端->目的端方向出现了问题，可以按照下面的方法确定出问题的节点，先从源端检查。

版权所有 © 华为技术有限公司

- 目的端->源端方向出现问题时方法一样，从目的端检查。

执行 **tracert** *dest-ip-address* 命令确定报文丢失的位置。

```
<Huawei> tracert 1.1.1.1
  traceroute to 1.1.1.1 (1.1.1.1), max hops: 30, packet length: 40, press CTRL_C to break
    1 30.1.1.1 5  ms  4 ms  3 ms
    2 89.0.0.2 10 ms  11 ms  8
    3   *  *  *
    .....
```

上面所示在 89.0.0.2 10 的下一跳设备（即显示为“3 * * *”的节点）出了问题。确定了出问题的设备后请执行步骤 5。

说明

Tracert VPN 时，请使用 **tracert -vpn-instance** *vpn-name destination-address* 来检测。其中的**-vpn-instance** *vpn-name* 是指 Tracert 目的地址所属的 VPN 实例。

步骤 5 检查出问题的节点上是否配置了本机防攻击策略

因有的设备有受到过 ICMP 报文的攻击，为了防止攻击，将 ICMP 报文上送 CPU 的速率改小或将 ICMP 报文直接丢弃（Drop），从而导致了 Ping 不通的情况。

使用命令 **display current-configuration | include cpu-defend**，检查设备配置文件中是否存在 **cpu-defend policy** 配置。

- 如果存在 CPU 防攻击策略，使用命令行 **display cpu-defend policy** *policy-number* 检查：
  - 是否配置了 Ping 相关 IP 地址的黑名单。
  - 是否配置了 CAR。如果配置了 CAR，请确认 CAR 的带宽参数是否过小，导致 Ping 报文无法处理。

  如果上述两种情况中的任何一种符合，都将导致 Ping 不通或丢包。请根据业务情况分析，如需继续执行 Ping 操作，请执行 undo 命令删除相应配置后再次执行 Ping 命令。如仍不能 Ping 通，请执行步骤 6。
- 如果没有配置 CPU 防攻击策略，请执行步骤 6。

步骤 6 在出问题的节点检查 FIB 和 ARP 表项是否正确

在出问题的节点执行 **display fib** *slot-number destination-address*，检查是否存在到目的地址的路由，如果路由不存在请参见 **7.4 OSPF 故障处理**或 IS-IS 故障处理进行处理。

如果路由存在并且报文所经链路是以太链路，请执行 **display arp**，查看所需的 ARP 表项是否存在，如果不存在请执行步骤 9，否则请执行步骤 7。

说明

对于 Ping VPN 的情况，请使用 **display fib** *slot-number* **vpn-instance** *vpn-name destination-address* 命令查看 FIB 表项。其中的 **vpn-instance** *vpn-name* 是指 Ping 目的地址所属的 VPN 实例。

步骤 7 在出问题的节点检查接口下是否存在错包

执行命令 **display interface** *interface-type interface-number*，查看接口的报文计数信息。检查如下信息：

以太网接口的显示信息中 CRC 计数在两次执行该命令之间是否有增长。

- 如果接口下错包或告警计数有增长，请排查链路和光模块问题。
- 如果接口下错包或告警计数没有增长，请继续执行步骤 8。

版权所有 © 华为技术有限公司

步骤 8 确定出问题的层面

请通过下面的方法和步骤在出问题的设备上继续定位出问题的层面：

1. 查看 ICMP 报文是否正常接收。

```
<Huawei> display icmp statistics
Input: bad formats       0     bad checksum               0
       echo              0     destination unreachable    0
       source quench     0     redirects                  0
       echo reply        0     parameter problem          0
       timestamp         0     information request        0
       mask requests     0     mask replies               0
       time exceeded     0
       Mping request     0     Mping reply                0
Output:echo              0     destination unreachable 476236
       source quench     0     redirects                  0
       echo reply        0     parameter problem          0
       timestamp         0     information reply          0
       mask requests     0     mask replies               0
       time exceeded     0
       Mping request     0     Mping reply                0
```

若没有收到 ICMP 报文，或是收到有错包，请执行步骤 9。

若 ICMP 报文接收正常，请执行子步骤 b。

2. 检查 IP 层面是否正常

通过 **display ip statistics** 命令查看 IP 层面的统计信息以确认是否是 IP 层面出了问题，如下所示：

```
<Huawei> display ip statistics
  Input:     sum               123174     local                  0
             bad protocol           0     bad format             0
             bad checksum           0     bad options            0
             discard srr            0     TTL exceeded           0
  Output:    forwarding             0     local             268816
             dropped                0     no route               0
  Fragment: input                   0     output                 0
             dropped                0
             fragmented             0     couldn't fragment      0
 Reassembling:sum                   0     timeouts               0
```

如果上面的统计信息显示的错误统计计数（如 bad protocol、 bad format、bad checksum、 bad options、discard srr、TTL exceeded、dropped、no route、couldn't fragment）有增加，那么就有表明有错误报文到达了 IP 层面，IP 经合法性判断后将其丢弃。

- 如果发生这种情况，说明本机的单板可能有故障，请执行步骤 9。
- 如果统计计数正常，请执行子步骤 c。

3. 查看 ICMP 报文是否从 IP 层正常下发

通过配置 ACL 的方式，确认报文是否下发到接口板。

ACL 配置文件举例如下：

```
acl number 3000
rule 5 permit icmp source 1.1.1.1 0 destination 1.1.1.2 0
```

打开 IP 报文的 debug 开关：

注意

打开 debug 开关会对系统性能造成一定影响，请确认后再操作。

```
<Huawei> debugging ip packet acl 3000
```


版权所有 © 华为技术有限公司

```
<Huawei> terminal monitor
<Huawei> terminal debugging
```

执行 Ping 操作，如 Ping 5 个报文。在终端上查看：是否显示发送了 5 个报文。如果没有看到发送 5 个报文，则说明 ICMP 报文没有下发到接口板。请执行步骤 9。

步骤 9 请收集如下信息，并联系华为技术工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

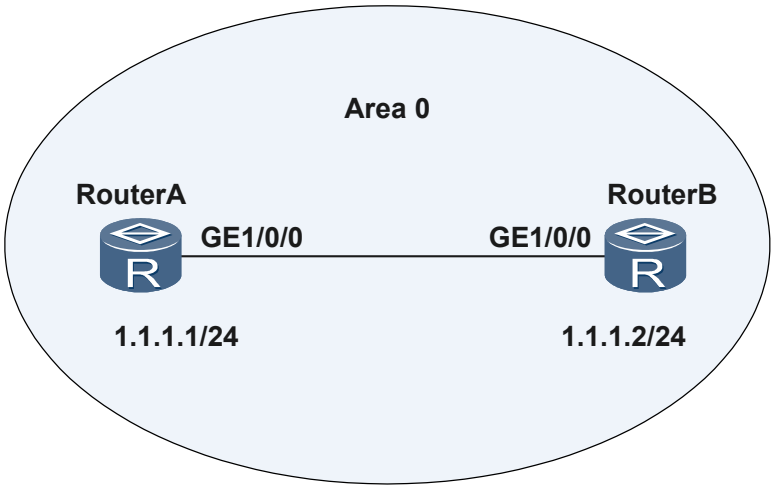
7.1.2 故障案例

错误的静态 ARP 表项导致直连设备两端不能 Ping 通

网络环境

用户用 RouterA 替换现网中设备,替换完成后组网图如图 7-3，替换完成后发现 RouterA 和 RouterB 无法正常 Ping 通。同时在 RouterA 查看 OSPF 状态为 Exchange，但是还原到替换之前的组网时一切恢复正常。

图 7-3 错误的静态 ARP 表项导致直连设备两端不能 ping 通的组网图



版权所有 © 华为技术有限公司

故障分析

1. 因为恢复之前的组网后一切正常，所以 RouterA 和 RouterB 之间的链路没有问题，RouterA 和 RouterB 之间是直连，因此不存在路由问题。RouterA 和 RouterB 不能正常 Ping 通有可能是 ARP 的学习问题。
2. 在 RouterA 上执行 **display arp all** 命令，检查 RouterA 是否学习到了 RouterB 的 ARP 表项。

```
<RouterA> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
1.1.1.1  0025-9e80-2494           I -         GE1/0/0
1.1.1.2  0025-9e80-248e  18       D-0         GE1/0/0
--------------------------------------------------------------------------------
Total:2        Dynamic:1       Static:0    Interface:1
```

发现 ARP 表项已经正常建立。

3. 在 RouterB 上执行 **display arp all** 命令，检查 RouterB 是否正常学习到了 RouterA 的 ARP 表项。

```
<RouterB> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
1.1.1.2  0025-9e80-248e           I -         GE1/0/0
1.1.1.1  0016-ecb9-0eb2  18       S          GE1/0/0
--------------------------------------------------------------------------------
Total:2        Dynamic:0       Static:1    Interface:1
```

输出信息显示 IP 地址 **1.1.1.1** 对应的 MAC 地址为 **0016-ecb9-0eb2**，表项类型“**S**”表示该 ARP 表项为静态配置。此时对比 RouterA 上的 ARP 表项发现，在 RouterB 上 **1.1.1.1** 对应的 MAC 地址并非 RouterA 上 **1.1.1.1** 对应的 MAC 地址。

因此，问题可能是 RouterB 在网络调整前配置了 IP+MAC+端口号的静态绑定，网络调整后因为对端的 MAC 变更，而 RouterB 上并未同步刷新 IP+MAC+端口号的静态 ARP，从而导致 RouterA 和 RouterB 无法正常 Ping 通。

操作步骤

步骤 1 在 RouterB 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **undo arp static** *ip-address mac-address*，删除当前错误的静态用户绑定表项。

说明

删除错误的静态 ARP 表项后，RouterA 和 RouterB 可以正常 Ping 通。这里通过配置静态用户绑定表项，能有效地防范网络中通过修改源地址而进行的恶意攻击行为。

步骤 3 执行命令 **arp static** *ip-address mac-address*，按照对端新加入的设备 MAC 地址配置正确的静态用户绑定表项。

完成上述步骤后 RouterA 和 RouterB 可以正常 ping 通。同时使用 **display ospf peer** 查看 OSPF 的邻居状态为“FULL”。

```
<RouterA> display ospf peer
        OSPF Process 1 with Router ID 11.11.11.105
                Neighbors

 Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/0)'s neighbors
 Router ID: 2.1.1.1              Address: 1.1.1.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 1.1.1.2  BDR: 2.1.1.1  MTU: 0
   Dead timer due in 30  sec
   Retrans timer interval: 5
```


版权所有 © 华为技术有限公司

```
Neighbor is up for 00:28:17
Authentication Sequence: [ 0 ]
```

----结束

案例总结

如果某设备上配置了 IP 和 MAC 地址的静态绑定，一旦该 MAC 地址对应设备被替换，则需要同步刷新静态绑定表项。此案例中如果 RouterB 的对端设备为其他厂商设备，在出现故障时无法正常登录设备查看对端设备配置，此时可以在 RouterA 上 PingRouterB，同时通过镜像抓包获取 RouterA 和 RouterB 之间的报文，然后对报文进行分析，从而判断报文中的目的 MAC 是否正确。

7.2 DHCP 故障处理

介绍 DHCP 常见故障的定位思路。

7.2.1 客户端无法获取 IP 地址的定位思路（AR2200-S 作为 DHCP Server）

AR2200-S 作为 DHCP Server 可以为同一个网段或不同网段内的客户端分配 IP 地址。

常见原因

本类故障的常见原因主要包括：

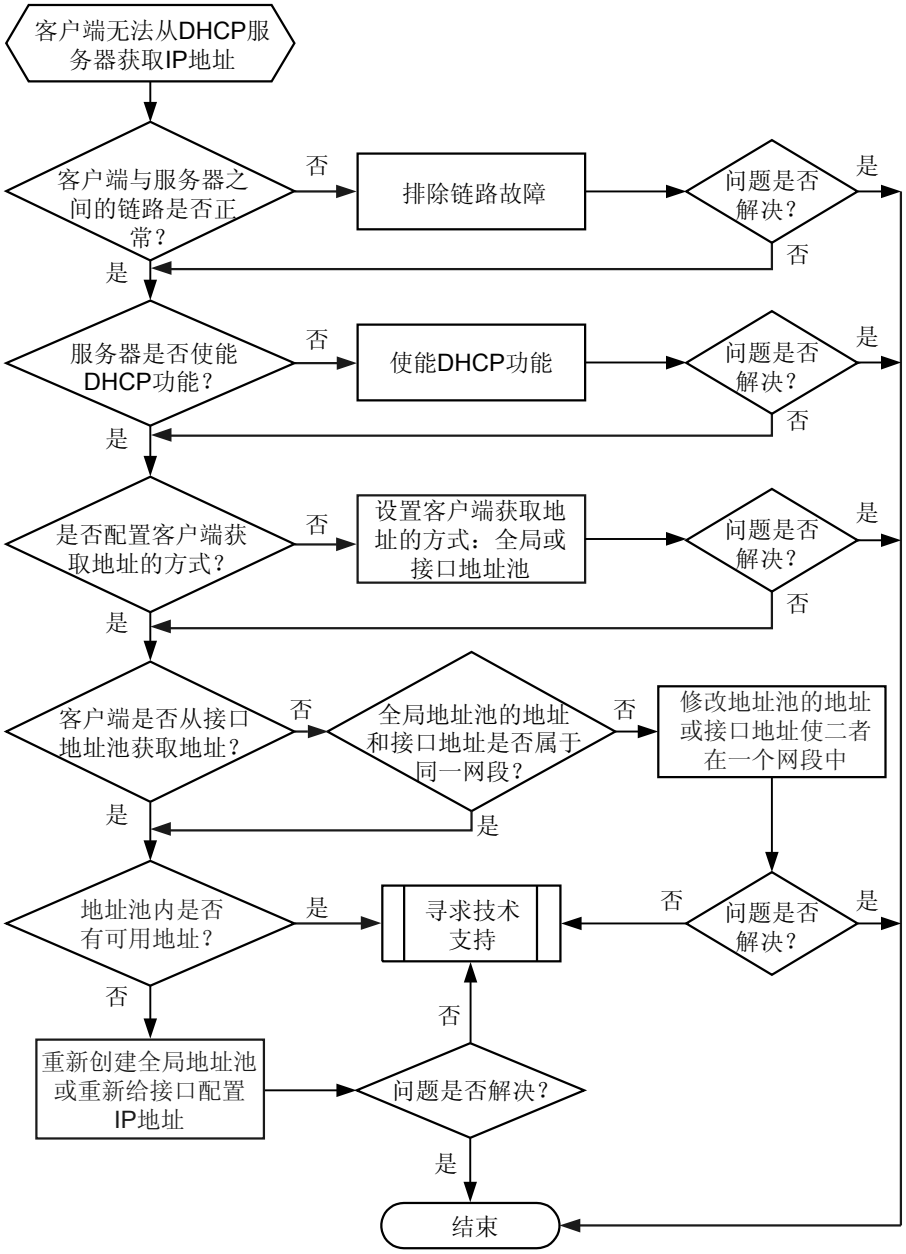
- 客户端与服务器之间的链路有故障。
- AR2200-S 未使能 DHCP 功能。
- AR2200-S 接口下没有选择 DHCP 分配地址的方式。
- 当选择从全局地址池中分配 IP 地址时：
  - 如果客户端与服务器在同一个网段内，全局地址池中的 IP 地址与 AR2200-S 接口的 IP 地址不在同一个网段中。
  - 如果客户端与服务器不在同一个网段内，中间存在中继设备时，全局地址池中的 IP 地址与中继设备接口的 IP 地址不在同一个网段中。
- 地址池中没有可用的 IP 地址可分配。

故障诊断流程

详细处理流程如图 7-4 所示。

版权所有 © 华为技术有限公司

图 7-4 客户端无法从 DHCP 服务器获取 IP 地址的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查客户端与 DHCP 服务器之间的链路是否有故障。

- 客户端与服务器在同一个网段内，在客户端与服务器连接的网卡上配置 IP 地址，确保该 IP 地址与服务器用户侧的接口的 IP 地址在同一网段，从客户端 Ping 服务器用户侧的接口的 IP 地址。

版权所有 © 华为技术有限公司

- 如果 Ping 不通，请先根据 **7.1 Ping 故障处理**排除链路的故障。
- 如果能 Ping 通，请执行步骤 2。

- 客户端与服务器不在同一个网段内，中间存在中继设备时，请分别 Ping 客户端与中继设备、中继设备与服务器之间的链路状态。
  - 如果 Ping 不通，请先根据 **7.1 Ping 故障处理**排除链路的故障。
  - 如果能 Ping 通，请执行步骤 2。

步骤 2 检查 DHCP 功能是否处于使能状态。

说明

如果未使能 DHCP 功能，则 AR2200-S 不会处理客户端上送的 DHCP 报文。

执行命令 **display current-configuration | include dhcp enable**，检查 DHCP 功能是否已经使能。缺省情况下，DHCP 功能未使能。

- 如果无任何 DHCP 相关显示信息，说明 DHCP 功能未使能，请执行命令 **dhcp enable**，使能 DHCP 功能。
- 如果显示 **dhcp enable**，说明 DHCP 功能已经使能，请执行步骤 3。

步骤 3 检查 AR2200-S 接口下是否选择 DHCP 分配地址的方式。

说明

如果 AR2200-S 接口下没有选择 DHCP 分配地址的方式，则客户端不能通过当前接口以 DHCP 的方式来获取 IP 地址。

在 AR2200-S 接口视图下，执行命令 **display this**，检查是否选择 DHCP 分配地址的方式。

显示信息	显示信息解释说明	后续操作
dhcp select global	接口已经选择全局地址池为 DHCP 客户端分配 IP 地址	请执行步骤 4
dhcp select interface	接口已经选择接口地址池为 DHCP 客户端分配 IP 地址	请执行步骤 5
无上述显示信息	接口没有选择 DHCP 分配地址的方式	执行命令 **dhcp select global** 或者 **dhcp select interface**，配置接口选择 DHCP 分配地址的方式。

步骤 4 检查全局地址池中的地址和接口地址是否属于同一个网段。

1. 执行命令 **display ip pool**，查看全局地址池是否存在。
   - 如果全局地址池不存在，执行命令 **ip pool** *ip-pool-name* 和命令 **network** *ip-address* [**mask** { *mask* | *mask-length* }]，创建全局地址池和配置全局地址池中可动态分配的 IP 地址范围。
   - 如果全局地址池存在，获取 *ip-pool-name* 参数值，执行步骤 b。
2. 执行命令 **display ip pool name** *ip-pool-name*，查看全局地址池中的 IP 地址是否与接口的 IP 地址在同一个网段中。
   - 客户端与服务器在同一个网段内：

版权所有 © 华为技术有限公司

- 如果全局地址池中的 IP 地址与 AR2200-S 接口的 IP 地址不在同一个网段中，则执行命令 **network** *ip-address* [**mask** { *mask* | *mask-length* }]重新配置全局地址池，使二者在一个网段中。
- 如果全局地址池中的 IP 地址与 AR2200-S 接口的 IP 地址在同一个网段中，请执行步骤 5。

● 客户端与服务器不在同一个网段内，中间存在中继设备时：
- 如果全局地址池中的 IP 地址与中继设备的接口的 IP 地址不在同一个网段中，则执行命令 **ip address** *ip address* 修改接口的 IP 地址，使二者在一个网段中。
- 如果全局地址池中的 IP 地址与中继设备的接口的 IP 地址在同一个网段中，请执行步骤 5。

步骤 5 检查地址池内是否有可用 IP 地址。

执行命令 **display ip pool name** *ip-pool-name*，检查全局/接口地址池中 IP 地址使用情况。

● 如果 **Idle（Expired）**值等于零，就说明地址池中的 IP 地址已经用尽。
- 如果接口选择全局地址池为 DHCP 客户端分配 IP 地址，可以重新创建一个全局地址池，该地址池的网段不能和前一个地址池的网段重叠，但网段可以相连。
- 如果接口选择接口地址池为 DHCP 客户端分配 IP 地址，可以重新为接口配置一个 IP 地址，该 IP 地址不能和前一个 IP 地址在同一个网段。

● 如果 **Idle（Expired）**值大于零，即存在可用的 IP 地址，请执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

● 上述步骤的执行结果。
● 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

7.2.2 客户端无法获取 IP 地址的定位思路（AR2200-S 作为 DHCP Relay）

客户端（DHCP Client）和 DHCP 服务器（DHCP Server）不在同一个网段内时，AR2200-S 作为 DHCP 中继（DHCP Relay）连接客户端和 DHCP 服务器，DHCP 服务器通过 DHCP 中继为客户端分配 IP 地址。

常见原因

本类故障的常见原因主要包括：

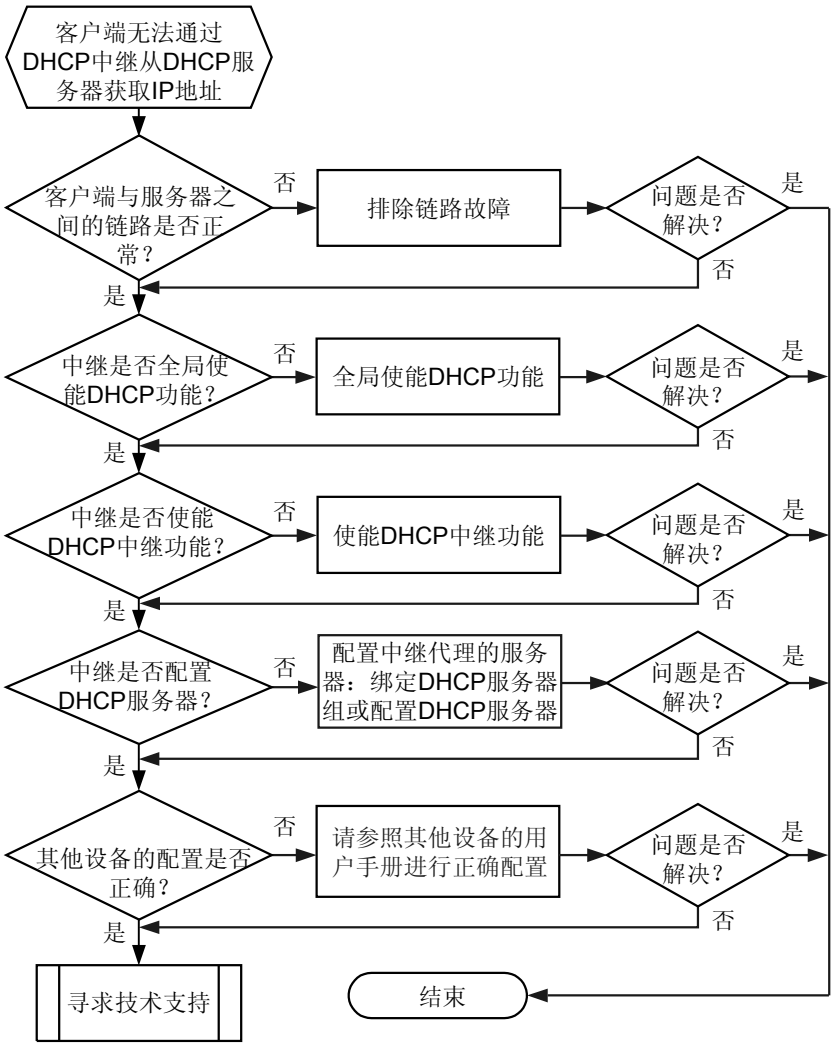
版权所有 © 华为技术有限公司

- 客户端与 DHCP 服务器之间的链路有故障。
  - 客户端与 DHCP 中继之间的链路有故障。
  - DHCP 中继与 DHCP 服务器之间的链路有故障。
- AR2200-S 未全局使能 DHCP 功能，导致 DHCP 功能没有生效。
- AR2200-S 未使能 DHCP 中继功能，导致 DHCP 中继功能没有生效。
- DHCP 中继没有配置所代理的 DHCP 服务器。
  - DHCP 中继没有配置所代理的 DHCP 服务器的 IP 地址。
  - DHCP 中继接口没有绑定 DHCP 服务器组，或者绑定的 DHCP 服务器组中没有配置所代理的 DHCP 服务器。
- 链路上其他设备配置错误。

故障诊断流程

详细处理流程如图 7-5 所示。

图 7-5 客户端无法通过 DHCP 中继从 DHCP 服务器获取 IP 地址的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查客户端与 DHCP 服务器之间的链路是否有故障。

1. 检查客户端和服务器之间是否有设备启用了 DHCP Snooping 功能。如果有，执行 **display dhcp snooping global** 命令查看全局 DHCP Snooping 的信息，确认连接 DHCP 服务器的接口是否配置为“信任”状态。
2. 检查客户端与 DHCP 中继之间的链路是否有故障。

   在客户端手工配置与 DHCP 中继用户侧接口位于同一网段的 IP 地址（不能与已经分配的 IP 地址冲突），然后在任一侧 ping 对端检查两者之间的链路是否有故障。

   - 如果 Ping 不通，请先根据 **7.1 Ping 故障处理**排除链路的故障。
   - 如果能 Ping 通，请执行步骤 c。
3. 检查 DHCP 中继与 DHCP 服务器之间的链路是否有故障。

   在 DHCP 中继上执行命令 **ping -a** *source-ip-address destination-ip-address*，*source-ip-address* 为 DHCP 中继用户侧接口的 IP 地址，*destination-ip-address* 为 DHCP 服务器的 IP 地址。

   - 如果 Ping 不通，请先根据 **7.1 Ping 故障处理**排除链路的故障。
   - 如果能 Ping 通，请执行步骤 2。

步骤 2 检查 DHCP 中继是否全局使能 DHCP 功能。

说明

如果未全局使能 DHCP 功能，则 AR2200-S 不会处理客户端上送的 DHCP 报文。

执行命令 **display current-configuration | include dhcp enable**，检查 DHCP 功能是否已经使能。缺省情况下，DHCP 功能未使能。

- 如果无任何显示信息，说明 DHCP 功能未使能，请执行命令 **dhcp enable**，使能 DHCP 功能。
- 如果显示 **dhcp enable**，说明 DHCP 功能已经使能，请执行步骤 3。

步骤 3 检查 DHCP 中继是否处于使能状态。

说明

- 如果 DHCP 中继未使能，则客户端无法跨网段来获取 IP 地址。
- 如果 AR2200-S 同时选择了 **global/interface** 和 **relay** 功能，则设备优先选择 DHCP Server 角色，当 DHCP Server 分配 IP 地址失败后，则会切换到 DHCP Relay 角色，开始 DHCP Relay 功能。

在 AR2200-S 接口视图下，执行命令 **display this**，检查 DHCP 中继是否处于使能状态。

- 如果显示 **dhcp select relay**，说明 DHCP 中继已经处于使能状态，请执行步骤 4。
- 如果无上述显示信息，说明 DHCP 中继处于未使能状态，请执行命令 **dhcp select relay**，使能 DHCP 中继功能。

步骤 4 检查 DHCP 中继是否配置了所代理的 DHCP 服务器。

版权所有 © 华为技术有限公司

说明

如果 DHCP 中继没有配置所代理的 DHCP 服务器，则没有 DHCP 服务器能够给该 DHCP 中继下的客户端分配 IP 地址。

在 AR2200-S 接口视图下，执行命令 **display this**，检查 DHCP 中继是否配置了所代理的 DHCP 服务器。

- 如果显示 **dhcp relay server-ip** *ip-address*，说明 DHCP 中继已经配置了所代理的 DHCP 服务器，请执行步骤 6。
- 如果显示 **dhcp relay server-select** *group-name*，说明 DHCP 中继的接口绑定了 DHCP 服务器组，请执行步骤 5。
- 如果无上述显示信息，说明 DHCP 中继没有配置 DHCP 服务器，请从以下两种配置方法中选择一种来配置 DHCP 服务器。
  - 请执行命令 **dhcp relay server-ip** *ip-address*，配置 DHCP 中继所代理的 DHCP 服务器地址。
  - 请执行命令 **dhcp relay server-select** *group-name*，绑定 DHCP 服务器组。执行命令 **dhcp-server**，在 DHCP 服务器组中添加 DHCP 服务器。

步骤 5 检查 DHCP 服务器组中是否配置了 DHCP 服务器。

说明

如果 DHCP 中继接口绑定了 DHCP 服务器组，但是该服务器组中没有配置 DHCP 服务器，同样没有 DHCP 服务器给该 DHCP 中继下的客户端分配 IP 地址。

执行命令 **display dhcp server group** *group-name*，检查 DHCP 服务器组中是否配置了 DHCP 服务器。

- 如果显示 **Server-IP** 字段，说明 DHCP 服务器组中配置了 DHCP 服务器，请执行步骤 6。
- 如果无上述显示字段，说明 DHCP 服务器组中没有配置 DHCP 服务器，请执行命令 **dhcp-server**，在 DHCP 服务器组中添加 DHCP 服务器。

步骤 6 检查链路上的其他设备，主要包括 DHCP 服务器、DSLAM、LAN Switch、客户端等设备。

请根据其他设备的用户手册检查相关配置是否正确，如不正确请修改相关配置。完成上述步骤后，如果客户端仍然无法获取 IP 地址，请执行步骤 7。

说明

其中 DHCP 服务器可以参考 **7.2.1 客户端无法获取 IP 地址的定位思路（AR2200-S 作为 DHCP Server）**检查服务器是否故障并排障。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

版权所有 © 华为技术有限公司

相关日志

无

7.3 RIP 故障处理

7.3.1 RIP 没有学到部分或全部路由的定位思路

常见原因

本类故障的常见原因主要包括：

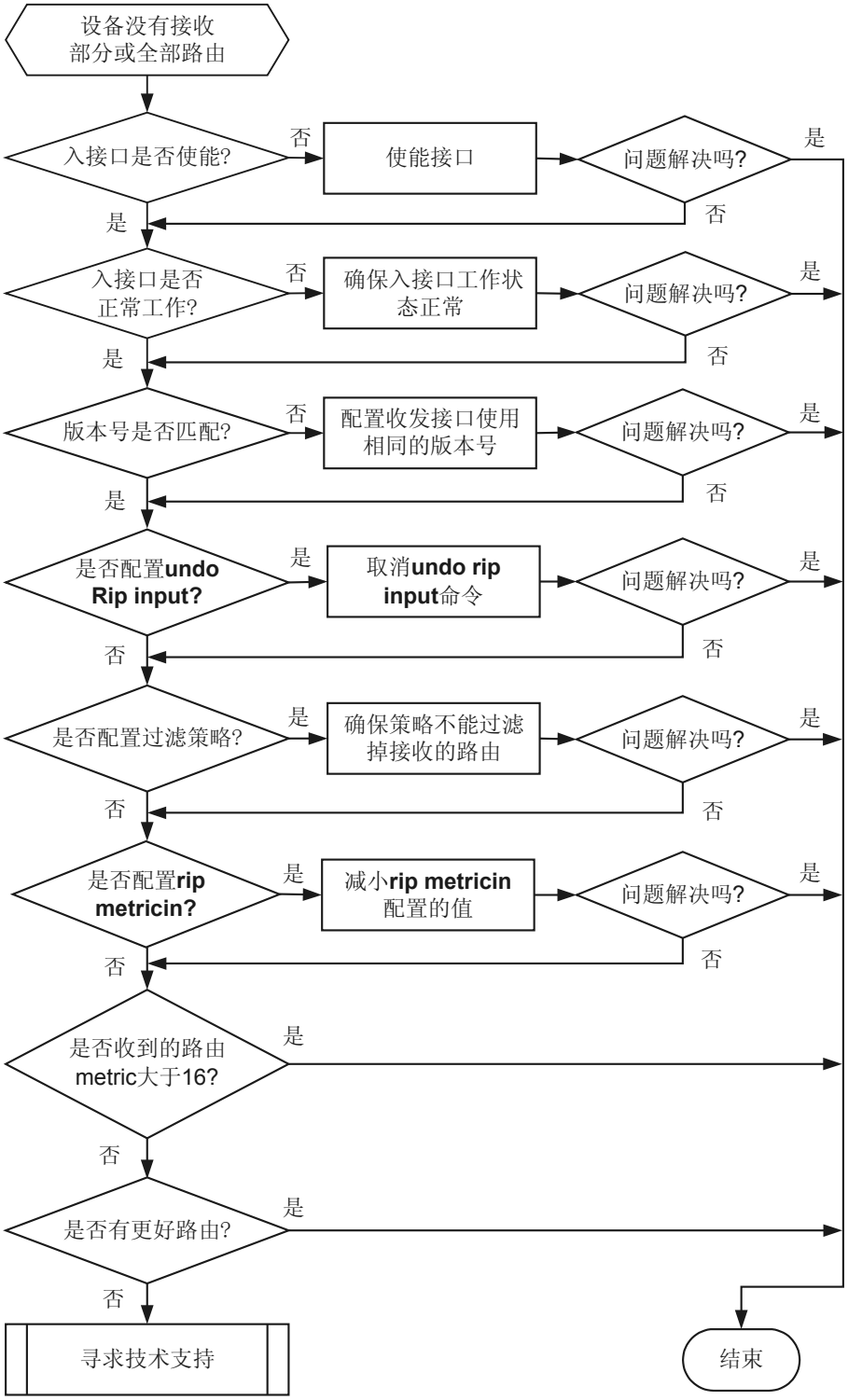
- 接口未使能 RIP
- 接口状态不是 Up
- 对端发送 RIP 协议报文的版本号和本地接口接收的 RIP 协议报文版本号不一致
- 接口上配置了禁止接收 RIP 报文
- 在 RIP 中配置了策略，过滤掉收到的 RIP 路由
- 收到的路由度量值大于 16
- 路由表中存在其它协议学到的相同路由
- 路由超限
- 入接口的 MTU 值小于 532
- 链路两端的接口认证方式不匹配。

故障诊断流程

在配置各路由器后，发现部分或全部路由没有接收，或 **display ip routing-table** 显示信息中没有 RIP 学到的路由。请使用下面的故障诊断流程，如图 7-6 所示。

版权所有 © 华为技术有限公司

图 7-6 RIP 路由接收故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查入接口是否在 RIP 中使能

network 命令用来使能指定接口网段，只有使能了 RIP 协议的接口才会进行 RIP 路由的接收、发送。使用命令 **display current-configuration configuration rip** 可以看到当前使能 RIP 的网段信息，检查入接口是否在其中。

network 命令使能的网络地址，必须是自然网段的地址。

步骤 2 检查入接口工作是否正常

使用 **display interface** 命令，查看入接口的工作状态：

- 如果接口当前物理状态为 Down 或 Administratively Down，那么 RIP 将无法从这个接口接收到路由。
- 如果接口当前协议状态为 Down，那么 RIP 已经从该接口学到的路由的 cost 值先变为 16，再被清除。

因此，必须确保接口的工作状态正常。

步骤 3 检查对方发送版本号和本地接口接收的版本号是否匹配

缺省情况下，接口只发送 RIP-1 报文，但可以接收 RIP-1 和 RIP-2 报文。当入接口与收到的 RIP 报文使用不同的版本号时，有可能造成 RIP 路由不能被正确的接收。

步骤 4 检查入接口是否配置了 **undo rip input** 命令

rip input 命令用来控制允许指定接口接收 RIP 报文。**undo rip input** 命令用来禁止指定接口接收 RIP 报文。如果在入接口配置了 **undo rip input**，则从这接口上来的 RIP 报文都得不到处理，导致收不到路由。

步骤 5 检查在 RIP 中是否配置了策略，过滤掉收到的 RIP 路由

filter-policy import 命令用来过滤接收的 RIP 路由信息。如果使用 ACL 过滤路由，通过命令 **display current-configuration configuration acl-basic** 可以查看从邻居来的 RIP 路由是否被过滤掉；如果使用 IP 地址前缀列表过滤路由，使用 **display ip ip-prefix** 查看配置策略。

如果被路由策略过滤掉，请正确地配置路由策略。

步骤 6 检查入接口是否配置了 **rip metricin** 命令，使得接收到得路由的度量值大于 16

rip metricin 命令用来设置接口接收 RIP 报文时给路由增加的度量值。如果最终的度量值超过了 16，则认为该路由不可达，从而不会将该路由加到路由表。

步骤 7 检查收到的路由度量值是否大于 16

同上，如果接收到的 RIP 路由的度量值超过 16，则认为该路由不可达，从而不会将该路由加到路由表。

版权所有 © 华为技术有限公司

步骤 8 检查链路两端的接口认证方式是否匹配

通过 **display rip** *process-id* **statistics interface** *interface-type interface-number* 查看接口的报文认证是否失败。

如果报文认证失败，请正确地配置认证方式。

步骤 9 检查在路由表中是否有其它协议学到的相同路由

通过 **display rip** *process-id* **route** 查看是否从邻居接收到了路由。可能的情况是：RIP 路由已经正确的接收了，同时本地还从其它的协议学到了相同的路由，比如 OSPF 或者 IS-IS。这时，OSPF 或 IS-IS 的协议权重一般大于 RIP，路由管理将优先选择通过 OSPF 或 IS-IS 学到的路由。通过命令 **display ip routing-table protocol rip verbose** 应该可以看到该路由，状态应该是非激活的。

步骤 10 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

7.3.2 设备没有发送部分或全部 RIP 路由的定位思路

常见原因

本类故障的常见原因主要包括：

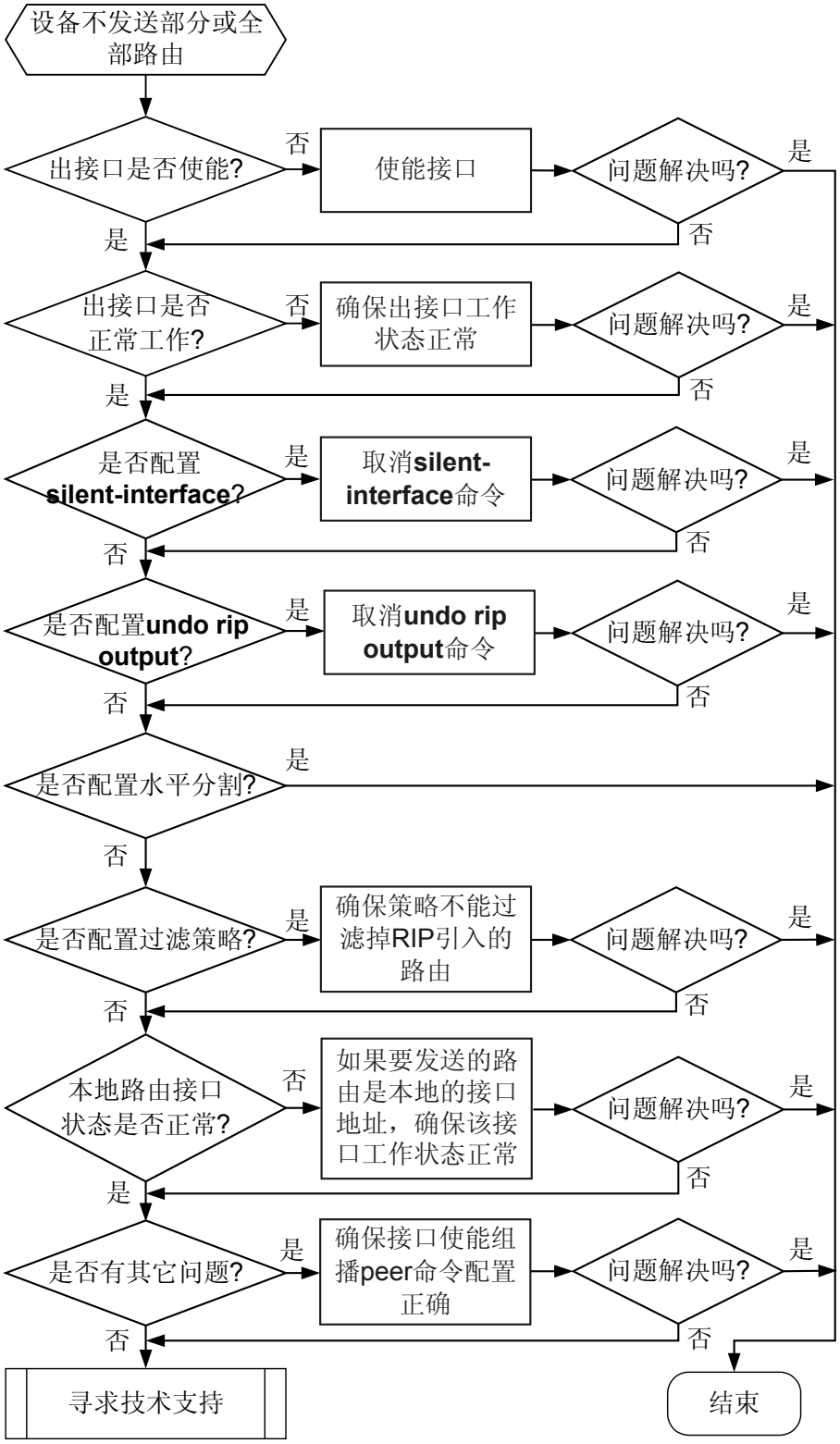
- 接口未使能 RIP
- 接口状态不是 Up
- 接口下配置了 **silent-interface** 命令，被抑制发送 RIP 报文
- 接口下配置了 **undo rip output** 命令，被禁止发送 RIP 报文
- 接口上没有使能水平分割
- RIP 中是否配置了策略，过滤掉引入到 RIP 的路由
- 端口的物理状态是“Down”或“Administratively Down”，或者接口出方向协议的当前状态是“Down”。因此，接口的 IP 地址不能够加到 RIP 的发布路由表中。
- 出接口不支持组播，而要发送的报文是发送到组播地址；或者如果出接口不支持广播，而要发送的报文是发送到广播地址
- 出接口的 MTU 值小于 52.

版权所有 © 华为技术有限公司

故障诊断流程

在配置各路由器后发现路由器不发送部分或全部路由。请使用下面的故障诊断流程，如图 7-7 所示。

图 7-7 RIP 路由发送故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查出接口是否在 RIP 中使能

network 命令用来使能指定接口网段，只有使能了 RIP 协议的接口才会进行 RIP 路由的接收、发送。使用命令 **display current-configuration configuration rip** 可以查看当前使能 RIP 的网段信息，检查入接口是否在其中。

network 命令使能的网络地址，必须是自然网段的地址。

步骤 2 检查出接口工作是否正常

使用 **display interface** 命令，查看出接口的工作状态。如果接口当前物理状态为 Down 或 Administratively Down，或者当前协议状态为 Down，那么 RIP 将不能在该接口上正常工作。因此，必须确保接口的工作状态正常。

步骤 3 检查出接口是否配置了 **silent-interface** 命令

silent-interface 命令用来抑制接口使其不发送 RIP 报文。使用命令 **display current-configuration configuration rip** 查看出接口是否被抑制。如果是，则取消对该接口的抑制。

步骤 4 检查出接口是否配置了 **undo rip output** 命令

在出接口上使用命令 **display current-configuration** 查看是否配置了 **rip output**。**rip output** 命令用来允许接口发送 RIP 报文。**undo rip output** 命令用来禁止接口发送 RIP 报文。如果显示出接口配置了 **undo rip output**，则将不能从该接口发送 RIP 报文。

步骤 5 检查出接口是否配置了水平分割命令

在出接口上使用命令 **display current-configuration** 查看是否配置了 **rip split-horizon**。缺省情况下，出接口都使能了水平分割，该命令的显示信息中没有关于水平分割的配置项；但对于 NBMA（NonBroadcast Multiple Access）网络连接的出接口（如 X.25、FR），如果没有显示关于水平分割的配置项，则表明在该接口上没有使能水平分割。

水平分割是指：从一个接口学到的路由，将不能再从该接口对外发布。水平分割机制是用于避免相临邻居间的路由循环。所以不要轻易取消接口的水平分割。

步骤 6 检查在 RIP 中是否配置了策略，过滤掉引入到 RIP 的路由

filter-policy export 命令用来配置全局出口过滤策略，只有通过过滤策略的路由才能被加入 RIP 的通告路由表中，并通过更新报文发布出去。

步骤 7 如果要发送的路由是本地的接口地址，检查该接口的状态

使用 **display interface** 命令，查看接口的工作状态。如果显示接口当前物理状态为 Down 或 Administratively Down，或者出接口的当前协议状态为 Down，则该接口的 IP 地址将不会被加入 RIP 的通告路由表。从而不会发给邻居。

版权所有 © 华为技术有限公司

步骤 8 检查是否有其它特殊问题

如果出接口不支持组播，而要发送的报文是发送到组播地址；或者如果出接口不支持广播，而要发送的报文是发送到广播地址，将会出现故障。这时候可以先排除接口的问题，然后在 RIP 模式下配置 **peer** 命令，使用单播地址进行发送，可以避免此故障发生。

步骤 9 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

7.4 OSPF 故障处理

7.4.1 OSPF 邻居 Down 的定位思路

常见原因

本类故障的常见原因主要包括：

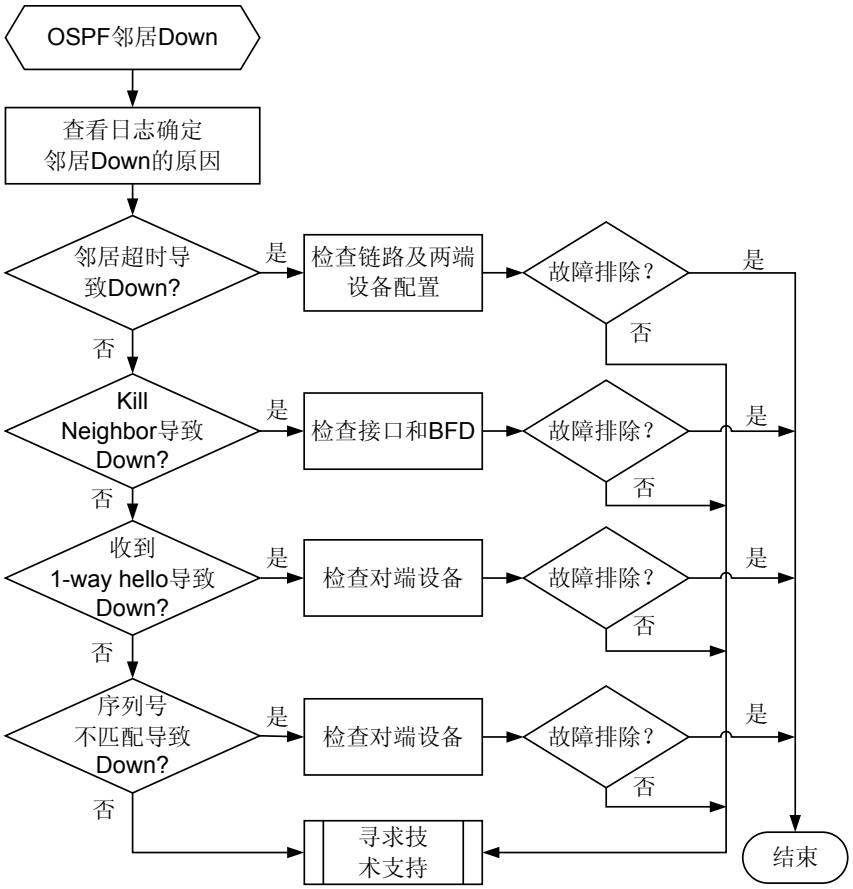
- BFD 故障。
- 对端设备故障。
- CPU 利用率过高。
- 链路故障。
- 接口没有 Up。
- 两端 IP 地址不在同一网段。
- RouterID 配置冲突。
- 两端区域类型配置不一致。
- 两端 OSPF 参数配置不一致。

故障诊断流程

在配置 OSPF 后发现 OSPF 邻居 Down，可按照故障诊断流程图 **7-8** 排除故障。

版权所有 © 华为技术有限公司

图 7-8 OSPF 邻居 Down 故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 通过日志查看 OSPF 邻居 Down 的原因

执行 **display logbuffer** 命令，查看如下日志信息。

```
NBR_DOWN_REASON(l): Neighbor state leaves full or changed to Down. (ProcessId=[USHORT],
NeighborRouterId=[IPADDR], NeighborAreaId=[ULONG], NeighborInterface=
[STRING],NeighborDownImmediate reason=[STRING], NeighborDownPrimeReason=[STRING],
NeighborChangeTime=[STRING])
```

重点关注关键字 NeighborDownImmediate reason，此关键字记录的是 OSPF 邻居 Down 的原因。OSPF 邻居 Down 的原因一般会有以下几种：

- Neighbor Down Due to Inactivity

  表示在 deadtime 时间内没有收到 Hello 报文导致 OSPF 邻居 Down，出现这种情况请执行**步骤 2**。

- Neighbor Down Due to Kill Neighbor

版权所有 © 华为技术有限公司

表示因为接口 Down、BFD Down 或执行了 **reset ospf process** 操作。此时，可以通过查看 NeighborDownPrimeReason 字段判断具体原因：

- 如果是 Physical Interface State Change 则表示接口状态发生了改变，请执行 **display interface** [*interface-type* [*interface-number*]]命令查看接口状态，排查接口故障。
- 如果是 BFD Session Down，则表示 BFD 会话状态变成 Down，请排查 BFD 故障。
- 如果是 OSPF Process Reset，则表示执行了 **reset ospf process** 的操作，OSPF 进程正在重启，请等待 OSPF 重新建立邻居关系。

- Neighbor Down Due to 1-Wayhello Received 或 Neighbor Down Due to SequenceNum Mismatch

  表示因为对端 OSPF 状态首先变成 Down，从而向本端发送 1-Wayhello，导致本端 OSPF 状态也变成 Down。这种情况请先排查对端设备的原因。

- 其他情况请执行**步骤 9**。

步骤 2 检查链路是否故障

请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**。

步骤 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 CPU 利用率 ROUT 字段值是否超过 60%。如果 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。如果 CPU 利用率超过 60%则执行**步骤 9**，否则执行**步骤 4**。

步骤 4 检查接口状态是否为 Up

请执行 **display interface** [*interface-type* [*interface-number*]]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 Down。接口在 OSPF 协议下正常状态可能为 DR、BDR、DROther 或 P2P 等。

```
<Huawei> display  ospf interface
            OSPF Process 1 with Router ID 1.1.1.1
                    Interfaces
Area: 0.0.0.0
IP Address      Type          State     Cost    Pri   DR              BDR
192.1.1.1       Broadcast     DR        1       1     192.1.1.1       0.0.0.0
```

- 如果接口在 OSPF 协议下状态为 Down，请执行命令 **display ospf cumulative** 检查 OSPF 进程下使能的接口数是否超出了规格，如果超出规格则减少 OSPF 使能的接口数。详细的规格请参见产品的 PAF/License 文件。

```
<Huawei> display ospf cumulative
          OSPF Process 1 with Router ID 1.1.1.1
                  Cumulations
  IO Statistics
             Type        Input     Output
            Hello            0         86
   DB Description            0          0
   Link-State Req            0          0
Link-State Update            0          0
   Link-State Ack            0          0
  SendPacket Peak-Control: (Disabled)
  ASE: (Disabled)
  LSAs originated by this router
  Router: 1
  Network: 0
  Sum-Net: 0
  Sum-Asbr: 0
  External: 0
  NSSA: 0
```


版权所有 © 华为技术有限公司

```
Opq-Link: 0
Opq-Area: 0
Opq-As: 0
LSAs Originated: 1  LSAs Received: 0
Routing Table:
  Intra Area: 1  Inter Area: 0  ASE: 0
Up Interface Cumulate: 1
```

- 如果接口在 OSPF 协议下状态不是 Down，请执行**步骤 5**。

步骤 5 如果接口连接的是广播网络或 NBMA 网络，检查两端 IP 地址是否在同一网段。

- 如果 IP 地址不在同一网段，请修改两端的 IP 地址，使其在同一网段。
- 如果 IP 地址处于同一网段，请执行**步骤 6**。

步骤 6 检查各接口的 MTU 是否一致

如果在接口上使能了 **ospf mtu-enable**，则要求接口的 MTU 一致，否则 OSPF 邻居无法协商成功。

- 如果接口的 MTU 值配置不一致，请在接口视图下执行 **mtu** *mtu* 命令，修改链路两端的 MTU 值为一致。
- 如果接口的 MTU 值配置一致，请执行**步骤 7**。

步骤 7 检查各接口的优先级是否非零

对于 Broadcast 和 NBMA 类型的网段，各接口的优先级至少有一个是非零的，以确保能够正确的选举出 DR，否则两边的邻居状态只能达到 2-Way。

执行命令 **display ospf interface**，查看接口的优先级。

```
<Huawei> display ospf interface
        OSPF Process 100 with Router ID 1.1.1.41
                Interfaces
Area: 0.0.0.0
IP Address      Type         State    Cost  Pri   DR             BDR
1.1.1.41        Broadcast    DR       1      1     1.1.1.41       0.0.0.0
```

步骤 8 检查两端 OSPF 的配置是否有错误

1. 检查两端 OSPF RouterID 配置是否相同

```
<Huawei> display ospf brief
         OSPF Process 1 with Router ID 1.1.1.1
                OSPF Protocol Information
```

如果相同则执行 **ospf router-id***router-id* 命令修改配置使 Router ID 在 AS 域内唯一，否则继续执行以下检查。

2. 检查两端 OSPF Area 配置是否一致

```
<Huawei> display ospf  interface
         OSPF Process 1 with Router ID 111.1.1.1
                 Interfaces
 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR             BDR
 111.1.1.1       Broadcast    BDR      1     1     111.1.1.2      111.1.1.1
```

如果不一致则修改配置使两端 OSPF Area 一致，否则继续执行以下检查。

3. 检查两端 OSPF 的其他配置是否一致

每 10 秒钟执行一次命令 **display ospf error**，持续 5 分钟。

```
<Huawei> display ospf error
         OSPF Process 1 with Router ID 1.1.1.1
                OSPF error statistics
General packet errors:
 0     : IP: received my own packet     0     : Bad packet
 0     : Bad version                    0     : Bad checksum
```


版权所有 © 华为技术有限公司

```
 0     : Bad area id                  0     : Drop on unnumbered interface
 0     : Bad virtual link             0     : Bad authentication type
 0     : Bad authentication key       0     : Packet too small
 0     : Packet size > ip length      0     : Transmit error
 0     : Interface down               0     : Unknown neighbor
HELLO packet errors:
 0     : Netmask mismatch             0     : Hello timer mismatch
 0     : Dead timer mismatch          0     : Extern option mismatch
 0     : Router id confusion          0     : Virtual neighbor unknown
 0     : NBMA neighbor unknown        0     : Invalid Source Address
```

- 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，需要在两端设备上执行 **area-authentication-mode** 命令配置相同认证的类型。
- 查看 **Hello timer 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 hello timer 配置不一致，需要通过检查两端设备接口配置，执行 **ospf timer hello** 命令将 hello timer 间隔配置一致。
- 查看 **Dead timer mismatch** 字段，如果这个字段对应的计数值一直在增长，表示接口的 dead timer 配置不一致，需要通过检查两端设备接口配置，执行 **ospf timer dead** 命令将 dead timer 间隔配置一致。
- 查看 **Extern 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），需要将两端区域类型配置一致（在 OSPF 区域视图下，如果有 **stub** 命令，表示区域类型为 stub；如果有 **nssa** 命令，表示区域类型为 nssa）。

如果故障仍然存在，请执行步骤 9。

步骤 9 请收集如下信息，并联系华为技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange

相关日志

OSPF/4/NBR_DOWN_REASON

7.4.2 OSPF 邻居无法达到 FULL 状态的定位思路

常见原因

本类故障的常见原因主要包括：

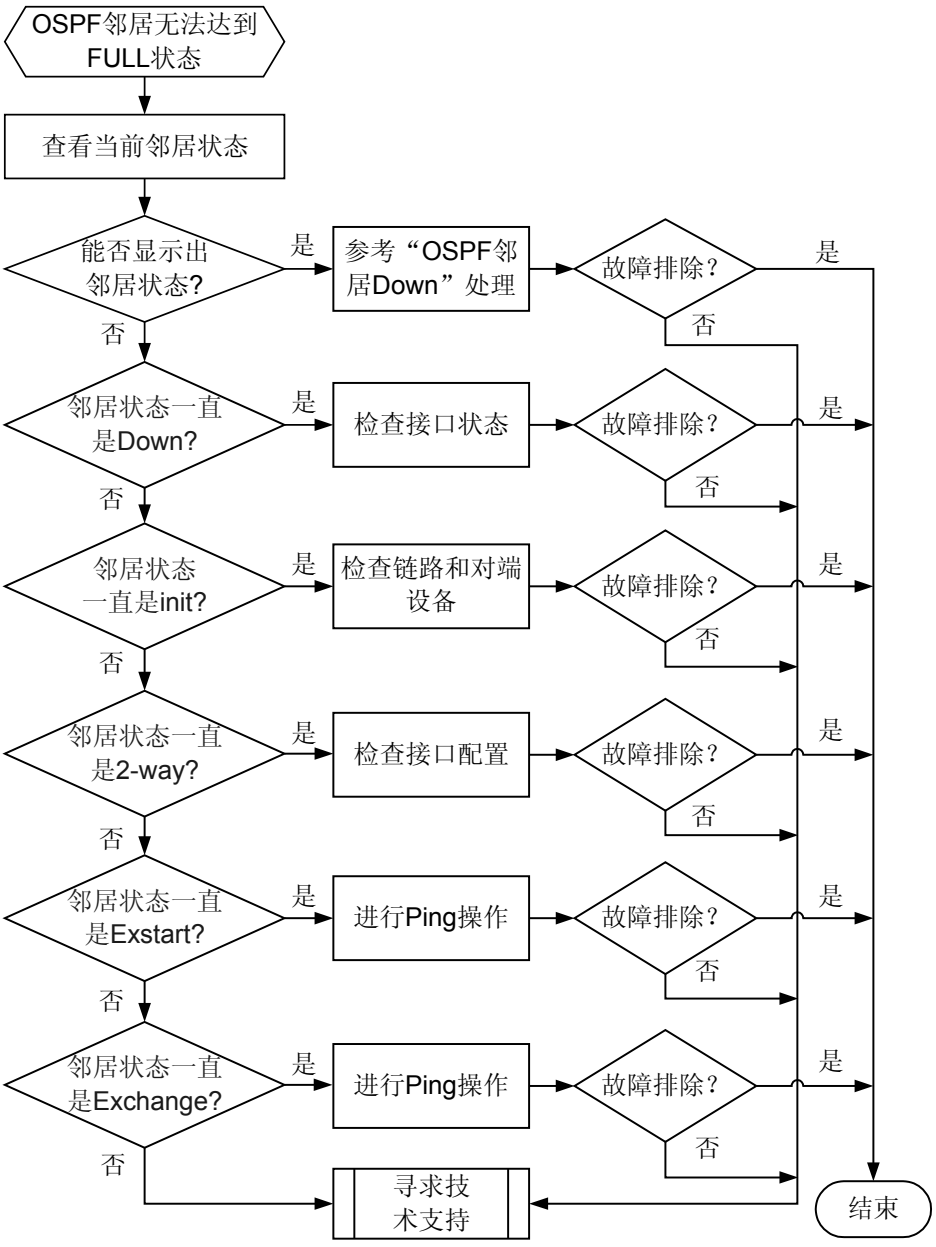
- 链路故障，OSPF 报文被丢弃。
- 接口的 dr-priority 配置不合理。
- 两端配置的 OSPF MTU 值不相等。

版权所有 © 华为技术有限公司

故障诊断流程

可按照故障诊断流程图 7-9 排除故障。

图 7-9 OSPF 邻居无法达到 FULL 状态故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 根据不同的邻居状态进行相应的处理

- 无法显示 OSPF 邻居

  如果查看邻居状态时显示不出 OSPF 邻居，请参见 **OSPF 邻居 Down 故障处理**。

- 邻居状态一直是 Down

  请执行 **display interface** [*interface-type* [*interface-number*]]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 Up（接口 Up 状态为 DR、BDR、DROther 或 P2P）。

```
<Huawei> display  ospf interface
          OSPF Process 1 with Router ID 1.1.1.1
                Interfaces
Area: 0.0.0.0
IP Address      Type          State     Cost    Pri   DR              BDR
192.1.1.1       Broadcast     DR        1       1     192.1.1.1       0.0.0.0
```

  - 如果 OSPF 下的接口为 Up，请执行**步骤 2**
  - 如果 OSPF 下的接口为 Down，请执行命令 **display ospf cumulative** 检查 OSPF 进程下使能的接口数是否超出了规格，如果超出规格则减少 OSPF 使能的接口数。

```
<Huawei> display ospf cumulative
         OSPF Process 1 with Router ID 1.1.1.1
                Cumulations
  IO Statistics
            Type        Input     Output
           Hello            0         86
    DB Description          0          0
    Link-State Req          0          0
Link-State Update           0          0
    Link-State Ack          0          0
  SendPacket Peak-Control: (Disabled)
  ASE: (Disabled)
  LSAs originated by this router
  Router: 1
  Network: 0
  Sum-Net: 0
  Sum-Asbr: 0
  External: 0
  NSSA: 0
  Opq-Link: 0
  Opq-Area: 0
  Opq-As: 0
  LSAs Originated: 1  LSAs Received: 0
  Routing Table:
    Intra Area: 1  Inter Area: 0  ASE: 0
  Up Interface Cumulate: 1
```

- 邻居状态一直是 init

  如果查看邻居状态时显示一直是 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。

- 邻居状态一直是 2-way

  如果查看邻居状态一直是 2-way，则执行命令 **display ospf interface** 查看设备在 OSPF 下面使能的接口配置的 dr-priority 是否为 0。

```
<Huawei> display ospf interface
          OSPF Process 1 with Router ID 111.1.1.1
                Interfaces

  Area: 0.0.0.0
  IP Address      Type          State     Cost  Pri   DR              BDR
  111.1.1.1       Broadcast     DROther   1     0     111.1.1.2       0.0.0.0
```


版权所有 © 华为技术有限公司

- 如果 OSPF 下使能的接口配置的 dr-priority 是 0 且 State 为 DROther，则说明他们都不是 DR 或 BDR，两者之间不需要交换 LSA，2-way 为正常状态，无需处理；
- 如果不是 0，请执行**步骤 2**

- 邻居状态一直是 Exstart

  如果查看邻居状态一直是 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：

  - 超大报文包无法正常收发

    可以通过执行命令 **ping -s** *1500 neighbor-address* 查看超大报文收发情况。如果无法 Ping 通，请先解决链路问题。

  - OSPF MTU 值配置不同

    如果 OSPF 接口下配置了 **ospf mtu-enable**，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

  如果查看邻居状态一直是 Exchange，表示设备在进行 DD 交换，请参见邻居状态一直是 init 状态处理。如果问题没有解决请执行**步骤 2**。

- 邻居状态一直是 Loading

注意

重启 OSPF 会导致该 OSPF 进程下所有邻居重新建立，并会导致业务暂时中断。

如果查看邻居状态一直是 Loading，可以尝试执行命令 **reset ospf** *process-id* **process** 重启 OSPF 进程。

如果问题没有解决请执行**步骤 2**。

步骤 2 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange

OSPF_1.3.6.1.2.1.14.16.2.8 ospfIfRxBadPacket

OSPF_1.3.6.1.2.1.14.16.2.16 ospfIfStateChange

相关日志

无

版权所有 © 华为技术有限公司

7.4.3 故障案例

OSPF 5 类 LSA FA 问题导致下挂设备路由不正常

网络环境

在图 7-10 的网络中，RouterC 是其他厂商设备，RouterA 和 RouterB 两台路由器上各有两个上行的 GE 接口，并分别配置两条静态路由，如下：

- RouterA

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 192.168.0.69
[RouterA] ip route-static 0.0.0.0 0.0.0.0 192.168.0.65
```

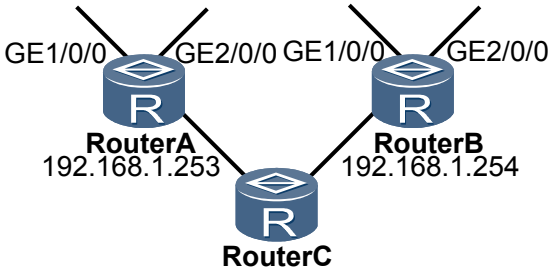
- RouterB

```
[RouterB] ip route-static 0.0.0.0 0.0.0.0 192.168.0.5
[RouterB] ip route-static 0.0.0.0 0.0.0.0 192.168.0.1
```

两台路由器都在 OSPF 进程中非强制发布默认路由给 RouterC，测试中发现 RouterC 上故障现象如下：正常时 RouterC 有两条 OSPF 默认外部路由指向两台路由器，但是如下两种情况时，RouterC 上只有一条 OSPF 默认路由指向两台路由器中的一台。

- 在 RouterA 上删除 192.168.0.65 的静态路由，其他保持不变。此时，在 RouterC 上只有一条 OSPF 默认路由指向 RouterB；
- 在 RouterB 上删除 192.168.0.1 的静态路由，其他保持不变。此时，RouterC 上只有一条 OSPF 默认路由指向 RouterA。

图 7-10 OSPF 5 类 LSA FA 问题导致下挂设备路由不正常组网图



故障分析

1. 在 RouterA 上执行 **undo ip route-static** *0.0.0.0 0.0.0.0 192.168.0.65*，然后在 RouterC 上查看对应 LSA 详细信息时，发现 FA 地址被 RouterA 置错，此时 RouterC 上只有一条 OSPF 默认路由指向 RouterB，因为 RouterC 上 OSPF 的 SPF 计算时发现 192.168.0.69 地址不可达。
2. 在 RouterB 上执行 **undo ip route-static** *0.0.0.0 0.0.0.0 192.168.0.1*，然后在 RouterC 上查看对应 LSA 详细信息时，发现 FA 地址被 RouterB 置错，此时 RouterC 上只有一条 OSPF 默认路由指向 RouterA，因为 RouterC 上 OSPF 的 SPF 计算时发现 192.168.0.5 地址不可达。
3. 从如上故障现象中，发现 RouterC 上出现 OSPF 路由学习不是预期的结果，根本的原因是上面 RouterA 和 RouterB 将 Forwarding Address（FA）设置错误。

   路由器填写 5 类 LSA 的 FA 地址及其路由计算的规则如下：

版权所有 © 华为技术有限公司

- FA 填写为 0.0.0.0 时：

  当一个 5 类 LSA 中的 FA 为 0.0.0.0 时，接收该 LSA 的路由器按照 Adv Rtr（也就是 ASBR）来计算下一跳。

- FA 填写为非 0.0.0.0 时：

  同时满足如下条件时，ASBR 会在 5 类 LSA 的 FA 域内填写非 0.0.0.0 的转发地址，接收 LSA 的路由器按照该非 0.0.0.0 地址计算下一跳。

  a. OSPF 在 ASBR 与外部网络连接的下一跳接口启动；

  b. ASBR 与外部网络连接的下一跳接口没有被设置为被动接口；

  c. ASBR 与外部网络连接的下一跳接口不是 OSPF P2P 或 P2MP 类型的；

  d. ASBR 与外部网络连接的下一跳接口地址是落在 OSPF 协议中发布的网络范围之内。

  不满足如上四点条件的，FA 都填写为 0.0.0.0。

操作步骤

步骤 1 如下几种方式可以解决此问题：

- 检查 RouterA 和 RouterB 的数据配置发现：
  - RouterA 上 OSPF 进程中配置了 **network** *192.168.0.68 0.0.0.3*，而没有配置 **network** *192.168.0.64 0.0.0.3*；
  - RouterB 上 OSPF 进程中配置了 **network** *192.168.0.4 0.0.0.3*，而没有配置 **network** *192.168.0.0 0.0.0.3*。

  分别在 RouterA 和 RouterB 上 OSPF 进程内，将对应静态路由下一跳网段的 **network** 配置删除，问题解决。
- 不影响正常业务的情况下，在 RouterA 和 RouterB 上 **network** 命令指定的接口下，分别执行 **ospf network-type p2p**，对端接口也如此修改，问题解决。
- 在 RouterA 和 RouterB 上将对应接口设置为 slience 接口，或者让 RouterA 和 RouterB 的所有静态路由的下一跳 IP 地址在 RouterC 上都是路由可达，都可以解决此问题。

----结束

案例总结

通过正确指定运行 OSPF 协议的接口的 IP 地址位于的网段和配置接口类型，使路由器必须按照规则填写 5 类 LSA 的 FA 地址及其路由计算。

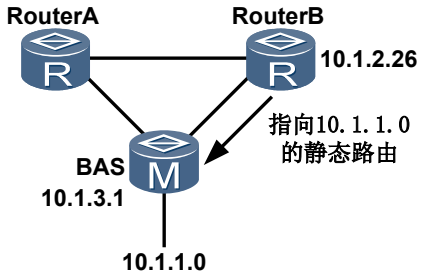
路由器收到两条相同 LSID 的 LSA 但其中一条不能计算出路由

网络环境

在图 7-11 的网络中，由于到 BAS 下的流量不均匀，需要让 RouterA 到 BAS 下目的网段的路由通过“RouterA--BAS--目的”和“RouterA--RouterB--BAS--目的”来形成负载分担均衡流量。

版权所有 © 华为技术有限公司

图 7-11 收到两条相同 LSID 的 LSA 但其中一条不能计算出路由组网图



下面以到目的网段为 10.1.1.0 为例。

用户在 RouterB 上配置了一条到 10.1.1.0 的静态路由，并且配置 OSPF 引入静态路由，RouterA 上收到 RouterB 发来的 LS ID 为 10.1.1.0 的 ASE LSA，同时 RouterA 上也收到从 BAS 发来的 LS ID 为 10.1.1.0 的 ASE LSA。结果，BAS 发来 LSA 生效计算出路由，RouterB 发来 LSA 并没有计算出路由。

故障分析

出现上述故障，可能有如下原因：

1. 配置问题。
2. RouterB 发来 LSA 中的 Forwarding Address: 10.1.2.26 置位，怀疑为 FA 问题导致 LSA 没被计算。
3. 生成负载分担路由条件不具备。

对上述原因进行一一排查和确认，结果如下：

1. 通过检查配置未发现问题。
2. 检查 FA 置位的 LSA，发现 LSA 符合计算路由条件。如下：

```
<RouterA> ping 10.1.3.1
  PING 10.1.3.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.3.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.1.3.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.1.3.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.1.3.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.1.3.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.1.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
<RouterA> display ip routing-table 10.1.3.1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.1.3.1/32  O_ASE   150  1           D   10.1.2.45     GigabitEthernet1/0/0
                  O_ASE   150  1           D   10.1.2.49     GigabitEthernet2/0/0
<RouterA> ping 10.1.2.26

    Reply from 10.1.2.26: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.1.2.26: bytes=56 Sequence=2 ttl=254 time=1 ms
```


版权所有 © 华为技术有限公司

```
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
<RouterA> display ip routing-table 10.1.2.26

    10.1.2.24/30  OSPF    10    101          D   10.1.2.45
GigabitEthernet1/0/0
                  OSPF    10    101          D   10.1.2.49       GigabitEthernet2/0/0
```

3. 在该网络中，LSA 的 cost 都是 1，则需要比较到 ASBR 的 cost 以及 FA 的 cost。

   对于 Type2 的 ASE LSA，OSPF 形成等价路由的比较方式如下：

   a. 比较 LSA 的 cost，如果相等，进行下一步比较；

   b. 比较到 ASBR/FA 的 cost，如果相等，形成等价路由。

   发现到 FA 转发地址的 cost 值为 101。

   - 对于 FA 为 0 的 LSA，其到 ASBR 10.1.3.1 的 cost 为 1；
   - 对于 FA 不为 0 的 LSA，其到 FA 10.1.2.26 的 cost 为 101；

   FA 置位的 LSA 由于优先级较低，所以没有被计算，因此无法形成等价路由。

操作步骤

步骤 1

此组网形成等价路由的办法为：

在 BAS 上，执行 **network** 命令使能 10.1.1.0 对应路由的下一跳。并执行 **ospf cost** 命令将该接口 cost 配置为 100，使其发布带 FA 的 LSA，FA 地址为接口地址。

这样在 RouterA 上，看到的两个 LSA 都有 FA，且到两个 FA 的 cost 都为 101，形成等价路由。

----结束

案例总结

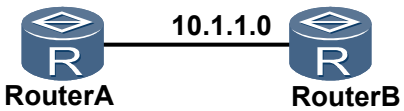
配置 OSPF 形成负载分担，需要正确配置带相同 FA 的 LSA，且配置 LSA 的相同 cost 值。

OSPF 邻居因链路问题无法建立

网络环境

在图 7-12 的组网中，RouterA 上 OSPF 邻居无法建立，状态为 State:Exchange。

图 7-12 OSPF 邻居因链路问题无法建立组网图



故障分析

出现上述故障，可能有如下原因：

版权所有 © 华为技术有限公司

- OSPF 配置问题。
- 两端设备的 OSPF 接口的相关参数不匹配。
- OSPF 协议报文被丢弃。

检查 RouterA 的 OSPF 配置，确认 RouterA 的 OSPF 配置没有问题。

检查两端设备的接口的 OSPF 相关参数，都匹配，也没有问题。

在 RouterB 上执行 **debugging ospf packet dd** 发现是 MTU 值协商不成功造成的。在两端设备上检查的 MTU 值都为 4470，但是 debug 信息发现 RouterB 收到的 MTU 值为“0”，即没有收到 RouterA 的 MTU 值。说明链路方面存在不畅通的情况。

在 RouterA 上 PING 对端设备直连接口地址，发现有丢包：

```
<RouterA> ping 10.1.1.0
  PING 10.1.1.0: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 10.1.1.0: bytes=56 Sequence=2 ttl=255 time=5 ms
    Reply from 10.1.1.0: bytes=56 Sequence=3 ttl=255 time=5 ms
    Reply from 10.1.1.0: bytes=56 Sequence=4 ttl=255 time=5 ms
    Request time out
  --- 10.1.1.0 ping statistics ---
    5 packet(s) transmitted
    3 packet(s) received
    40.00% packet loss
```

首先经过传输侧确认中间的链路没有问题。然后在 RouterA 上做流量统计，发现数据包是在 RouterA 接口之外丢掉的，也就是说数据包有可能是在对端设备单板上或者链路上丢掉的。

经过在对端设备上做流量统计，确认为 RouterB 单板问题。

操作步骤

步骤 1 更换 RouterB 的故障单板。

----结束

案例总结

有时 OSPF 的报文无法正确接收，原因有很多，首先要检查链路层是否畅通。可以打开 OSPF 的 debug 开关来查。Debug 命令有 **debugging ospf packet**、**debugging ospf event** 等，还可以通过 **display ospf error** 来看各种 OSPF 的错误统计信息。如果 OSPF 的信息正确，可以通过打开 **debugging ip packet** 来检查 IP 层是否转发成功。

Router-ID 冲突导致 OSPF 路由环路

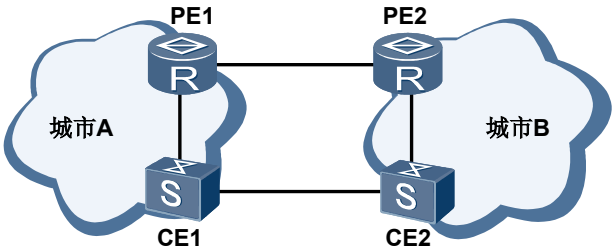
网络环境

在图 7-13 的组网中，PE 和 CE 之间运行 OSPF 多实例，CE 为其他厂商的三层交换机，PE 下发 OSPF 缺省路由引导两地业务的互通。

现象：本地 CE1 和 CE2 设备 PING 本地直连 PE 都正常，但是 PING 远端的 CE 和业务 IP 会出现偶尔不规则的丢包。

版权所有 © 华为技术有限公司

图 7-13 Router-ID 冲突导致 OSPF 路由环路组网图



故障分析

1. 由于在两边 PE 绑定的 VPN 实例中，10.1.1.33 为最大的一个 IP 地址。并且 OSPF 多实例的配置为：

   ```
   <PE1> ospf 4 vpn-instance www
   ```

   所以导致 PE1、PE2 的 OSPF 进程 4 都选择 10.1.1.33 做为 Router-ID。
2. 在 CE1、CE2 上查看两边 PE 的 Router-ID 都为 10.1.1.33。
3. 在 CE 上查看 debug 相关信息后发现，Router-ID 为 10.1.1.33 的设备不断发送 LSA，频率为 5 秒一次，而且 seq 值递增，不稳定。
4. CE 交换机均收到相同 Router-ID 的两台设备发送的 LSA，所以查看路由表看到的 OSPF 缺省路由信息就会不断变动。而当 CE1 的缺省路由从 CE2 中学到，CE2 的缺省路由又从 CE1 中学到时，就形成了路由环路，因此出现路由不可达，造成丢包。

操作步骤

步骤 1 在两台 PE 上分别执行命令，强制指定该 OSPF 多实例的 Router-ID 为 PE 本机上唯一的地址。

```
[PE1] ospf 4 router-id 10.2.2.9 vpn-instance www
[PE2] ospf 4 router-id 10.2.2.10 vpn-instance www
```

步骤 2 重启两台 PE 上设备该 VPN 实例的 OSPF 进程，业务恢复。

----结束

案例总结

建议在 PE 上强制指定 OSPF 多实例的 Router-ID 为 PE 本机上唯一的地址。

版权所有 © 华为技术有限公司

8 组播类

关于本章

8.1 三层组播故障处理

版权所有 © 华为技术有限公司

8.1 三层组播故障处理

8.1.1 组播业务不通的定位思路

常见原因

本类故障的常见原因主要包括：

- 路由配置错误；
- 因为接口状态不正确引起的组播流量不通；
- 协议表项未生成；
- 组播转发表项未生成。

故障诊断流程

在配置三层组播使能后发现组播业务不通。

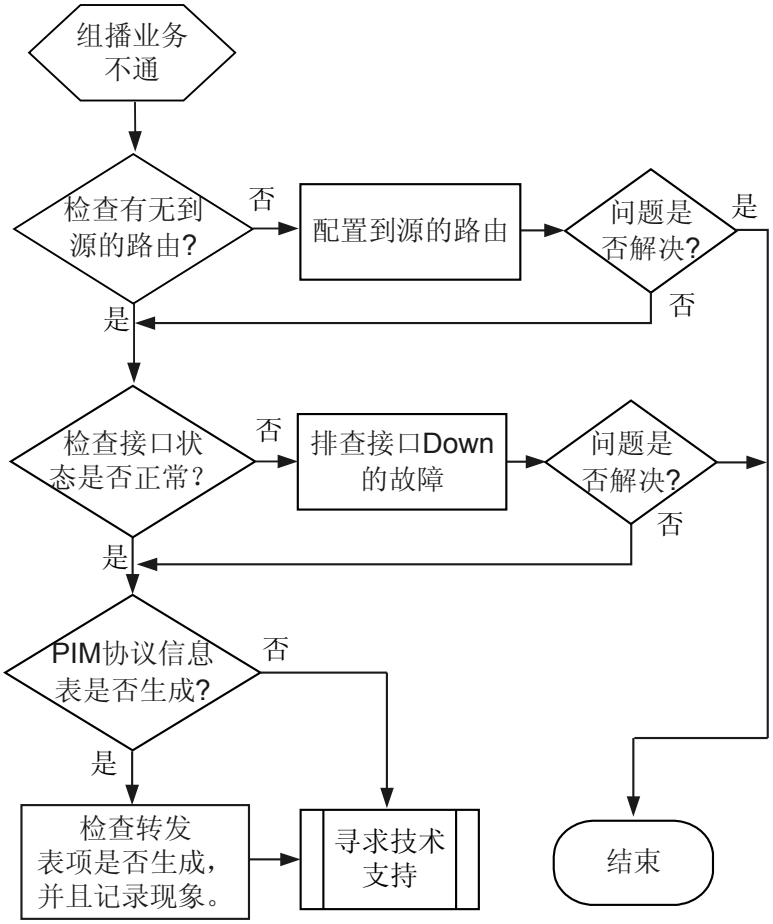
故障的定位思路如下：

- 检查有无到源的路由。
- 检查组播路由出、入接口状态是否正常。
- 检查 PIM 协议信息表是否生成。
- 检查转发表项是否生成。

详细处理流程如**图 8-1** 所示。

版权所有 © 华为技术有限公司

图 8-1 组播业务不通故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查有无到源的路由。

在设备上执行命令 **display ip routing-table** *ip-address*，查看本端路由表中是否有到源的路由。

说明

这里的参数 ip-address 指组播源地址。

- 如果没有到源的可达路由，请配置到源的路由。
- 如果本设备上有到源的路由，请执行步骤 2。

步骤 2 检查组播转发表项出、入接口的状态是否正常。

执行 **display interface** 命令，检查接口状态是否正常。

版权所有 © 华为技术有限公司

- 如果组播转发表项出、入接口的状态不正常，则组播转发表项无法生成，请先排除接口状态 Down 的故障。

  如下显示 GigabitEthernet2/0/0 的状态为 UP：

```
<Huawei>display interface GigabitEthernet 2/0/0
GigabitEthernet2/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, GigabitEthernet2/0/0 Interface
Switch Port,PVID :  200,The Maximum Frame Length is 1628
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-0005
Last physical up time   : 2008-01-31 19:19:06
Last physical down time : 2008-01-31 19:12:01
Current system time: 2008-02-04 16:18:20
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 128 bits/sec, 0 packets/sec
Last 300 seconds output rate 648 bits/sec, 0 packets/sec
Input peak rate 736 bits/sec,Record time: 2008-01-31 19:05:00
Output peak rate 1624 bits/sec,Record time: 2008-01-31 19:19:26

Input:  11177 packets, 4996374 bytes
  Unicast:                0,  Multicast:              11177
  Broadcast:              0,  Jumbo:                      0
  Discard:                0,  Total Error:                0

  CRC:                    0,  Giants:                     0
  Jabbers:                0,  Throttles:                  0
  Runts:                  0,  DropEvents:                 0
  Alignments:             0,  Symbols:                    0
  Ignoreds:               0,  Frames:                     0

Output:  194443 packets, 26925040 bytes
  Unicast:                0,  Multicast:             183273
  Broadcast:          11170,  Jumbo:                      0
  Discard:                0,  Total Error:                0

  Collisions:             0,  ExcessiveCollisions:        0
  Late Collisions:        0,  Deferreds:                  0
  Buffers Purged:         0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  : 0.01%
    Output bandwidth utilization : 0.01%
```

- 如果接口状态正常，请执行步骤 3。

步骤 3 检查 PIM 协议信息表是否生成。

在设备上执行 **display pim routing-table** 命令，检查上层协议表项是否生成。

- 如果没有表项显示，请直接联系华为技术支持工程师。
- 如果有表项显示，请执行步骤 4。

步骤 4 检查转发表项是否生成。

在设备上执行 **display multicast forwarding-table** 和命令，检查转发表项是否生成。

- 如果转发仍然不通，请记录显示结果，并联系华为技术支持工程师。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警与日志

相关告警

无

相关日志

无

8.1.2 PIM 邻居 Down 的定位思路

常见原因

本类故障的常见原因主要包括：

- 接口物理状态或协议状态为 Down
- 接口没有使能 PIM
- 接口的 PIM 相关配置不正确

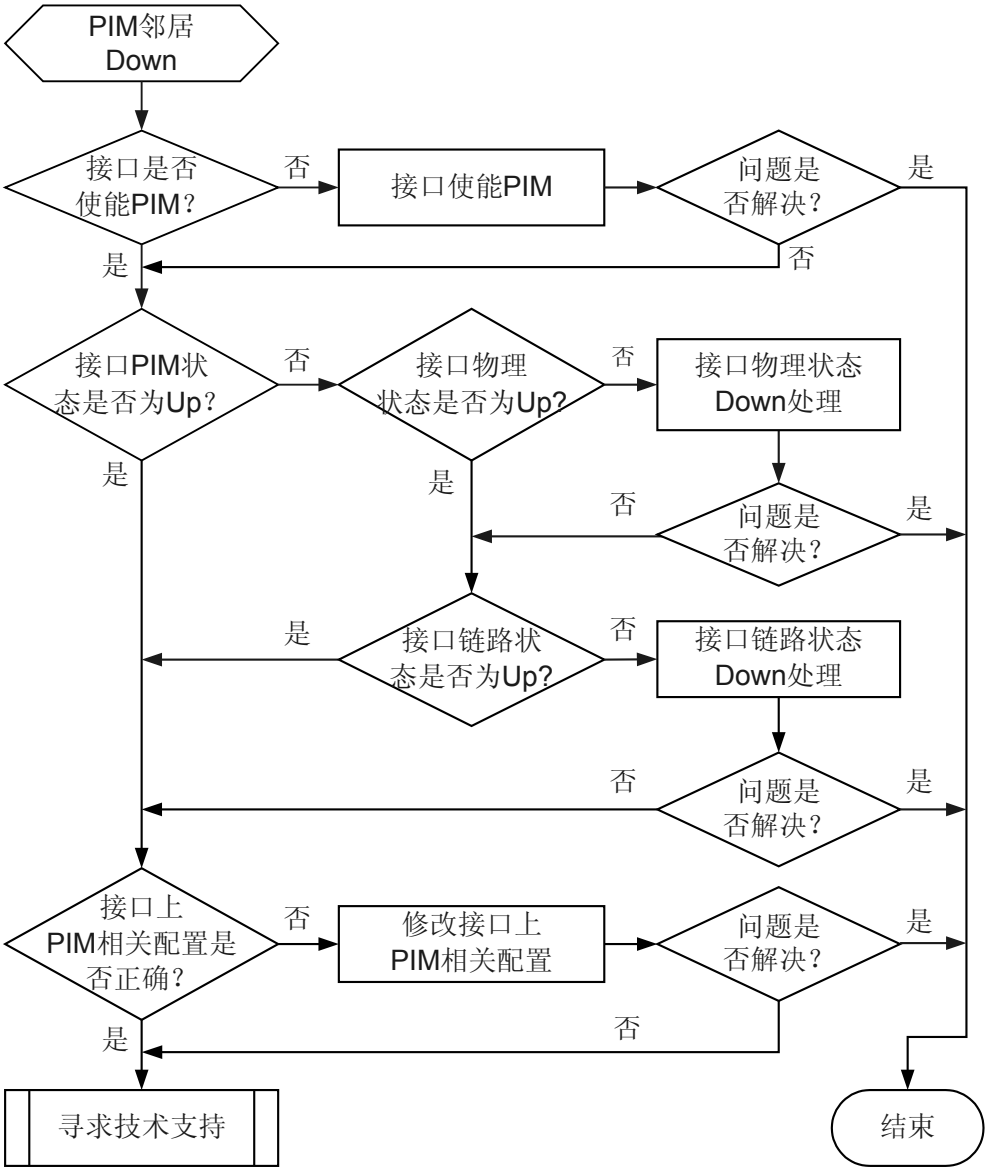
故障诊断流程

在配置 PIM 网络完成后发现 PIM 邻居 Down。

可按照故障诊断流程图 8-2 排除故障。

版权所有 © 华为技术有限公司

图 8-2 PIM 邻居 Down 故障诊断流程图



故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查接口是否使能 PIM

在设备上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口是否使能了 PIM。

版权所有 © 华为技术有限公司

- 如果接口上没有使能 PIM，则需要使能 PIM。

  如果接口使能 PIM 时出现提示信息：“Warning: Please enable multicast routing in the system view first”，则首先在系统视图下执行 **multicast routing-enable** 命令使能组播功能。然后在接口上使能 PIM-SM 或 PIM-DM。
- 如果接口已经使能 PIM，请执行步骤 2。

步骤 2 检查接口 PIM 状态是否为 Up

在设备上执行 **display pim interface** *interface-type interface-number* 命令，查看接口 PIM 状态是否为 Up。

- 如果接口 PIM 状态为 Down，请在设备上执行 **display interface** *interface-type interface-number* 命令查看接口的物理状态和链路状态是否为 Up。
  1. 如果物理状态没有 Up，请处理物理状态没有 Up 的问题。
  2. 如果是链路状态没有 Up，请处理链路状态没有 Up 的问题。
- 如果接口 PIM 状态为 Up，请执行步骤 3。

步骤 3 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 邻居关系的常见原因如下：

- 直连接口的 IP 地址没有配置在同一网段内。
- 接口配置了 PIM Silent。
- 接口配置了 PIM 邻居过滤策略，而 PIM 邻居的地址被过滤策略过滤掉了。
- 接口配置了拒绝接收无 Generation ID 参数的 Hello 消息，而 PIM 邻居发送的 Hello 消息中无 Generation ID 参数，导致 PIM 邻居无法建立。这种情况常见于与其他厂商设备互通场景。

在设备上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口上的 PIM 配置是否存在以上问题。

- 如果是由于以上原因导致的 PIM 邻居 Down，请修改接口上 PIM 相关配置。
- 如果检查结束，故障仍无法排除，请执行步骤 4。

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

PIM/4/NBR_DOWN

8.1.3 PIM-SM 网络中 RPT 无法正常转发数据的定位思路

版权所有 © 华为技术有限公司

常见原因

本类故障的常见原因主要包括：

- 组播设备到 RP 的单播路由不通
- 各组播设备的 RP 地址不一致
- 组播设备的下游接口没有收到（*，G）加入
- 接口没有使能 PIM-SM
- 到 RP 的 RPF 路由不正确（举例：单播路由环路）
- 配置问题（举例：TTL、MTU 或组播边界配置不当等）

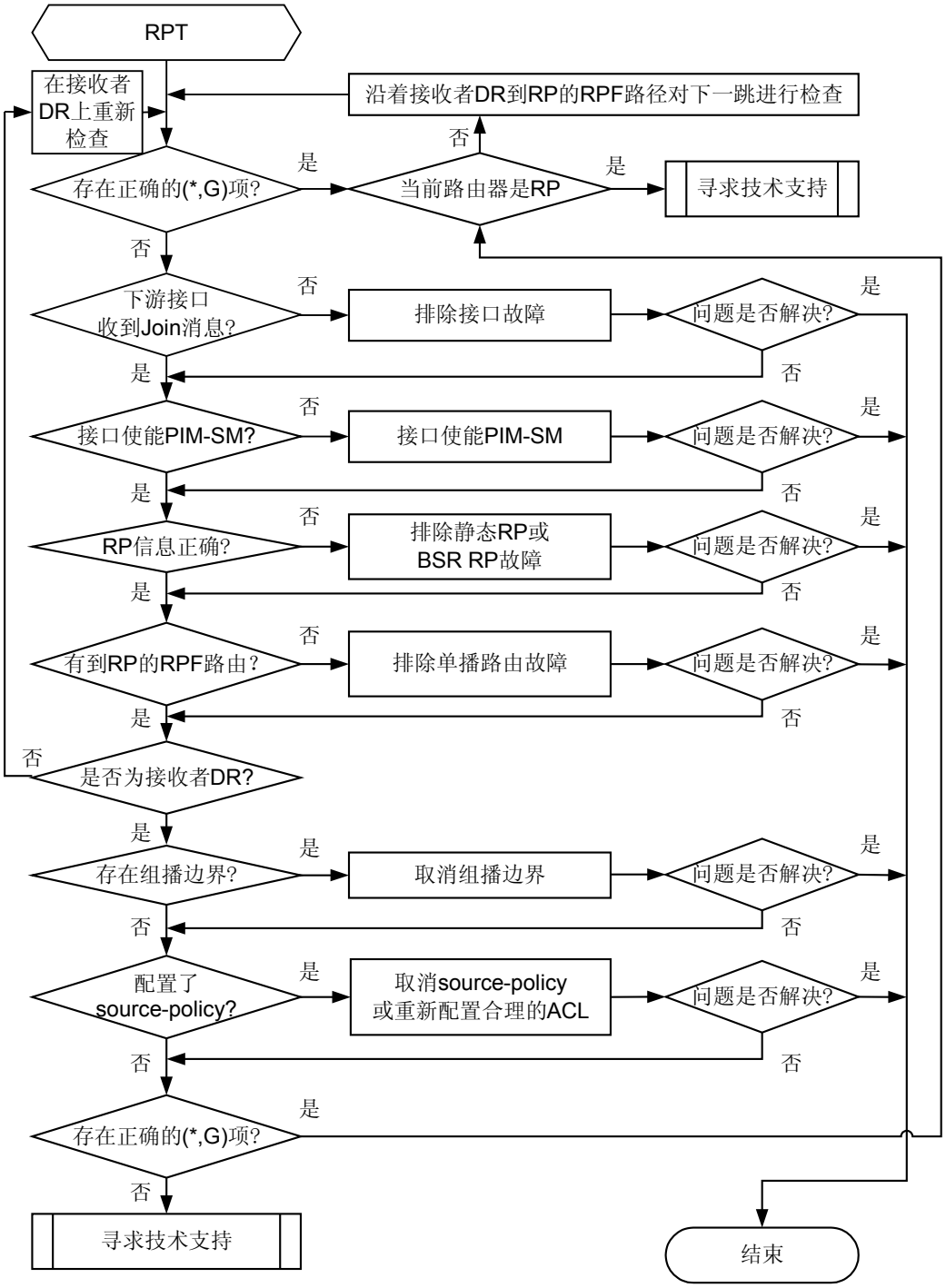
故障诊断流程

在配置 PIM-SM 网络后发现 RPT 无法正常转发数据。

可按照故障诊断流程图 8-3 排除故障。

版权所有 © 华为技术有限公司

图 8-3 PIM-SM 网络中 RPT 无法正常转发数据故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

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** *group-address* 命令，查看 PIM 路由表中是否存在正确的（*,G）表项。请重点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，则每隔 15 秒执行 **display multicast forwarding-table** *group-address* 命令，查看查转发表中是否存在与（*,G）表项相同组播组的（S,G）表项，并查看显示信息中的“Matched”计数是否保持增长。
  - 如果转发表中存在（S,G）表项且“Matched”计数保持增长，则表明上游设备到此设备的组播数据转发正常，但是由于某种原因导致无法向下游转发，可能是由于数据报文的 TTL 过小或转发问题。
  - 如果转发表中不存在（S,G）表项或“Matched”计数停止：
    - 如果当前设备不是 RP，则表明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。
    - 如果当前设备已经是 RP，则表明 RPT 已成功建立，但由于某种原因导致 RP 未收到组播源发出的组播数据。故障可能是由于源 DR 没有注册成功，请执行步骤 10。
- 如果 PIM 路由表中不存在正确的（*,G）表项，请执行步骤 2。

步骤 2 检查下游接口是否收到 Join 消息

在设备上执行 **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** 命令，查看下游接口收到的 Join/Prune 报文计数是否增加。

- 如果下游接口收到的 Join/Prune 报文计数没有增加，在下游设备上执行 **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** 命令，查看下游是否向上游发出了 Join/Prune 报文。
  - 如果计数增加，则表明下游已经发出了 Join/Prune 报文，则 PIM 邻居间通信有问题，请执行步骤 10。
  - 如果计数没有增加，则下游设备有问题，请排查下游设备的故障。
- 如果下游接口收到的 Join/Prune 报文计数增加，请执行步骤 3。

步骤 3 检查接口是否使能 PIM-SM

以下接口未使能 PIM-SM 是常见的故障原因：

- 到达 RP 的 RPF 邻居接口
- 到达 RP 的 RPF 接口
- 直连用户主机网段的接口（接收者 DR 的下游接口）

在设备上执行 **display pim interface verbose** 命令，查看接口的 PIM 信息。请重点检查上述接口是否使能 PIM-SM。

- 如果显示信息中缺失设备的某接口信息或某接口的 PIM 模式为 Dense，建议在该接口上配置 **pim sm**。

  如果在接口上使能 PIM-SM 时出现提示信息：“Warning: Please enable multicast routing first”，则首先在系统视图下使用 **multicast routing-enable** 命令使能组播功能。然后在接口上使能 PIM-SM。

版权所有 © 华为技术有限公司

- 如果设备的所有接口均已使能 PIM-SM，请执行步骤 4。

步骤 4 检查 RP 信息是否正确

在设备上执行 **display pim rp-info** 命令，查看设备是否已经学习到了为某组播组服务的 RP 信息，并且与其它所有设备为此组播组服务的 RP 信息一致。

- 如果设备上没有 RP 信息或 RP 信息与其他设备不同：
  - 如果网络中使用静态 RP，请执行 **static-rp** 命令在所有设备上将为某组播组服务的 RP 地址配置为一致。
  - 如果网络中使用动态 RP，请执行步骤 10。
- 如果所有设备为某组播组服务的 RP 信息已保持一致，请执行步骤 5。

步骤 5 检查是否存在到达 RP 的 RPF 路由

在设备上执行 **display multicast rpf-info** *source-address* 命令，查看是否存在到达 RP 的 RPF 路由。

- 如果显示信息中不存在到 RP 的 RPF 路由，检查单播路由配置。请在设备与 RP 上分别执行 **ping** 命令，检查是否能够 ping 通对方。
- 如果显示信息中存在到 RP 的 RPF 路由：
  - 如果显示信息表明 RPF 路由为组播静态路由，执行 **display current-configuration** 命令查看组播静态路由配置是否合理。
  - 如果显示信息表明 RPF 路由为单播路由，执行 **display ip routing-table** 命令查看单播路由是否与 RPF 路由一致。
- 如果显示信息中存在到 RP 的 RPF 路由，且路由配置合理，请执行步骤 6。

步骤 6 检查转发组播数据的接口是否为接收者 DR

在设备上执行 **display pim interface** *interface-type interface-number* 命令，查看转发组播数据的接口是否为接收者 DR。

- 如果显示信息中没有 local 标记，请根据显示信息中的 DR 地址在 DR 设备上按此处理步骤定位故障。
- 如果显示信息中有 local 标记，请执行步骤 7。

步骤 7 检查接口是否配置组播边界

在设备上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口是否配置了组播边界。

- 如果某接口的配置信息中出现“multicast boundary”，表明该接口配置了组播边界。建议执行 **undo multicast boundary** { *group-address* { *mask* | *mask-length* } | **all** } 命令删除该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。
- 如果接口没有配置组播边界，请执行步骤 8。

步骤 8 检查是否配置了 source-policy

在设备上执行 **display current-configuration configuration pim** 命令，查看 PIM 视图下的当前配置信息。

- 如果配置信息中出现“source-policy acl-number”，则表明配置了源过滤规则。如果接收到的组播数据不在 ACL 允许的范围之内，则将被丢弃。建议执行 **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。

版权所有 © 华为技术有限公司

- 如果没有配置 source-policy，请执行步骤 9。

步骤 9 检查 PIM 路由表是否存在正确的（*,G）表项

在设备上执行 **display pim routing-table** *group-address* 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。

步骤 10 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

8.1.4 PIM-SM 网络中 SPT 无法正常转发数据的定位思路

常见原因

本类故障的常见原因主要包括：

- 组播设备的下游接口没有收到（S，G）加入
- 接口没有使能 PIM-SM
- 到组播源的 RPF 路由不正确（举例：单播路由环路）
- 配置问题（举例：TTL、MTU、切换阈值或组播边界配置不当等）

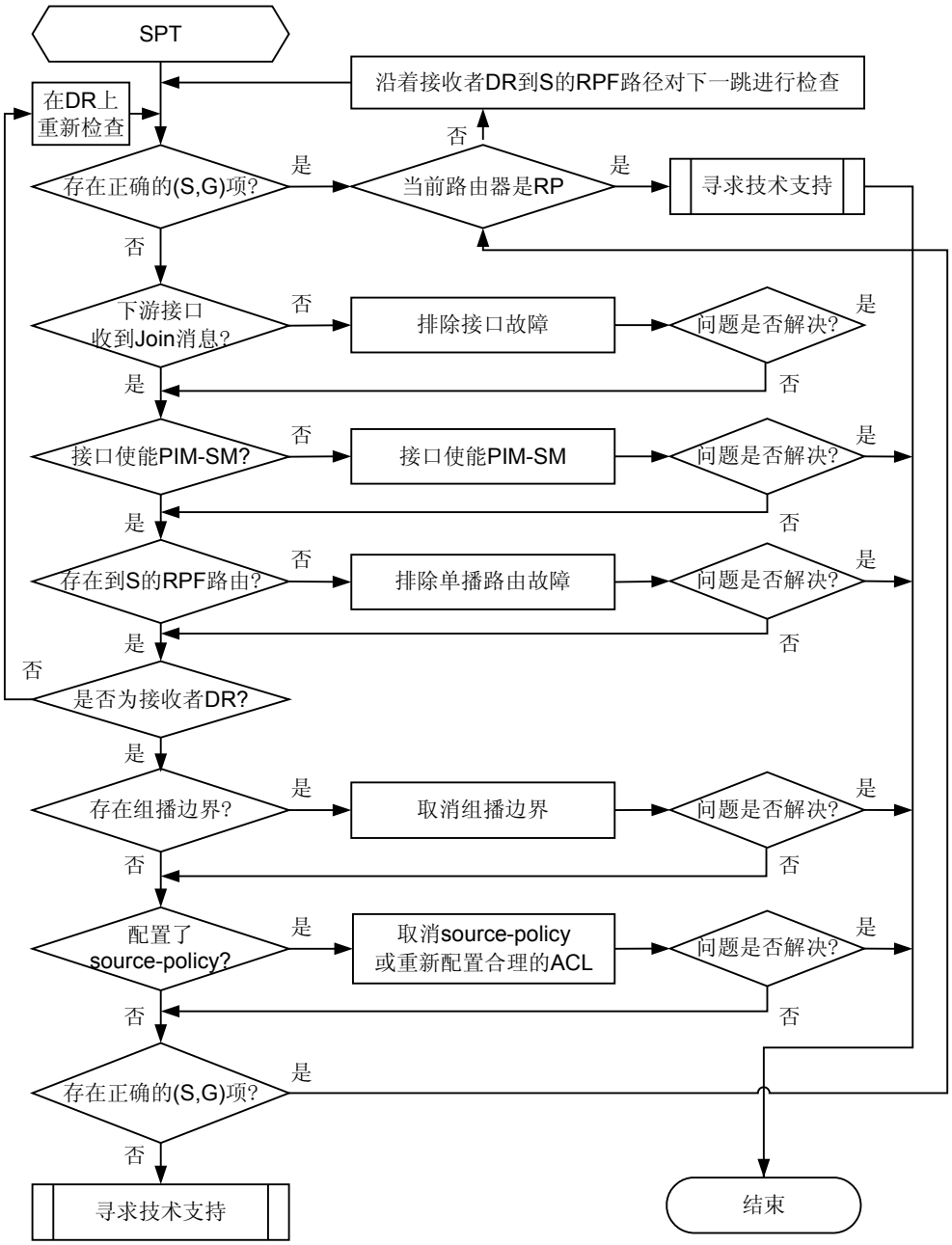
故障诊断流程

在配置 PIM-SM 网络后发现 SPT 无法正常转发数据。

可按照故障诊断流程图 8-4 排除故障。

版权所有 © 华为技术有限公司

图 8-4 PIM-SM 网络中 SPT 无法正常转发数据故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 PIM 路由表中是否存在正确的（S,G）表项

版权所有 © 华为技术有限公司

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，请执行 **display multicast forwarding-table** 命令查看转发表中的（S,G）表项并且查看显示信息中的“Matched”计数是否保持增长。转发计数更新较慢，执行 **display multicast forwarding-table** 命令后，由于计数更新比较慢，请等待几分钟。
    - 如果“Matched”计数保持增长，则表明上游设备到当前设备的组播数据转发正常，但是由于某种原因导致组播数据无法向下游设备转发。请执行步骤 9。
    - 如果“Matched”计数停止：
      - 如果当前设备不是源 DR，表明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 路由表中不存在正确的（S,G）表项，则按照此故障处理步骤排查上游设备的故障。
        - 如果上游设备的 PIM 路由表中存在正确的（S,G）表项，但“Matched”计数停止，请执行步骤 9。
      - 如果当前设备已是源 DR，则表明 SPT 已成功建立，但是由于某种原因导致源 DR 未沿 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。

步骤 2 检查下游接口是否收到 Join 消息

说明

如果当前设备是接收者 DR，请跳过此步骤。

下游接口没有收到对应的（S,G）Join 报文，可能的故障原因是：

- 该下游接口发生故障
- 该下游接口未使能 PIM-SM 协议

在设备上执行 **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** 命令，查看下游接口收到的 Join/Prune 报文计数是否增加。

- 如果下游接口收到的 Join/Prune 报文计数没有增加，在下游设备上执行 **display pim control-message counters interface** *interface-type interface-number* **message-type join-prune** 命令，查看下游是否向上游发出了 Join/Prune 报文。
  - 如果计数增加，则表明下游已经发出了 Join/Prune 报文，则 PIM 邻居间通信有问题，请执行步骤 9。
  - 如果计数没有增加，则下游设备有问题，请排查下游设备的故障。
- 如果下游接口收到的 Join/Prune 报文计数增加，请执行步骤 3。

步骤 3 检查接口是否使能 PIM-SM

在以下接口没有使能 PIM-SM 是常见的故障原因：

- 到达组播源的 RPF 邻居接口
- 到达组播源的 RPF 接口

版权所有 © 华为技术有限公司

说明

部署 PIM-SM 网络时，建议在网络中所有设备上使能组播，在所有接口上使能 PIM-SM 协议。

在设备上执行 **display pim interface verbose** 命令，查看接口上的 PIM 信息。请重点查看上述接口是否配置 PIM-SM。

- 如果显示信息中缺少设备的某接口信息或者某接口的 PIM 模式为 Dense，请在该接口上配置 **pim sm**。

  如果在接口上使能 PIM-SM 时出现提示信息：“Warning: Please enable multicast routing first”，请首先在系统视图下执行 **multicast routing-enable** 命令使能组播功能。然后在接口视图下执行 **pim sm** 命令使能 PIM-SM。
- 如果设备的所有接口均已使能 PIM-SM，请执行步骤 4。

步骤 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** *source-address* 命令，查看是否存在到达组播源的 RPF 路由。

- 如果显示信息中不存在到 RP 的 RPF 路由，检查单播路由配置。建议在设备与 RP 上分别执行 **ping** 命令，检查是否能够 ping 通对方。
- 如果显示信息中存在到 RP 的 RPF 路由：
  - 如果显示信息表明 RPF 路由为组播静态路由，执行 **display current-configuration** 命令，查看组播静态路由配置是否合理。
  - 如果显示信息表明 RPF 路由为单播路由，执行 **display ip routing-table** 命令，查看单播路由是否与 RPF 路由一致。
- 如果显示信息中存在到 RP 的 RPF 路由，且路由配置合理，请执行步骤 5。

步骤 5 检查转发组播数据的接口是否为接收者 DR

在设备上执行 **display pim interface** *interface-type interface-number* 命令，查看转发组播数据的接口是否为接收者 DR。

- 如果显示信息中没有 local 标记，请根据显示信息中的 DR 地址在 DR 设备上按此故障处理步骤定位故障。
- 如果显示信息中有 local 标记，请执行步骤 6。

步骤 6 检查接口是否配置组播边界

在设备上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口是否配置了组播边界。

- 如果某接口的配置信息中出现“multicast boundary”，表明该接口配置了组播边界。建议执行 **undo multicast boundary** { *group-address* { *mask* | *mask-length* } | **all** } 命令删除该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。
- 如果接口没有配置组播边界，请执行步骤 7。

步骤 7 检查是否配置了 source-policy

在设备上执行 **display current-configuration configuration pim** 命令，查看 PIM 视图下的当前配置信息。

版权所有 © 华为技术有限公司

- 如果配置信息中出现“source-policy acl-number”，则表明配置了源过滤规则。如果接收到的组播数据不在 ACL 允许的范围之内，则将被丢弃。建议执行 **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。
- 如果没有配置 source-policy，请执行步骤 8。

步骤 8 检查 PIM 路由表是否存在正确的（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（S,G）表项。具体方法请参见步骤 1。

步骤 9 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

8.1.5 MSDP 对等体无法正确建立（S,G）表项的定位思路

常见原因

本类故障的常见原因主要包括：

- 发起 SA 消息的 MSDP 对等体没有部署在 RP 上
- 部署 Anycast RP 的设备没有配置逻辑 RP 或逻辑 RP 配置错误
- 同一 Mesh Group 内的 MSDP 对等体没有两两建立对等体关系
- 域内组播协议采用的不是 PIM-SM
- 到组播源的 RPF 路由不正确（举例：单播路由环路）
- 配置问题（举例：SA-Policy、import-policy、TTL、切换阈值或组播边界配置不当等）
- SA 消息没有通过 RPF 检查

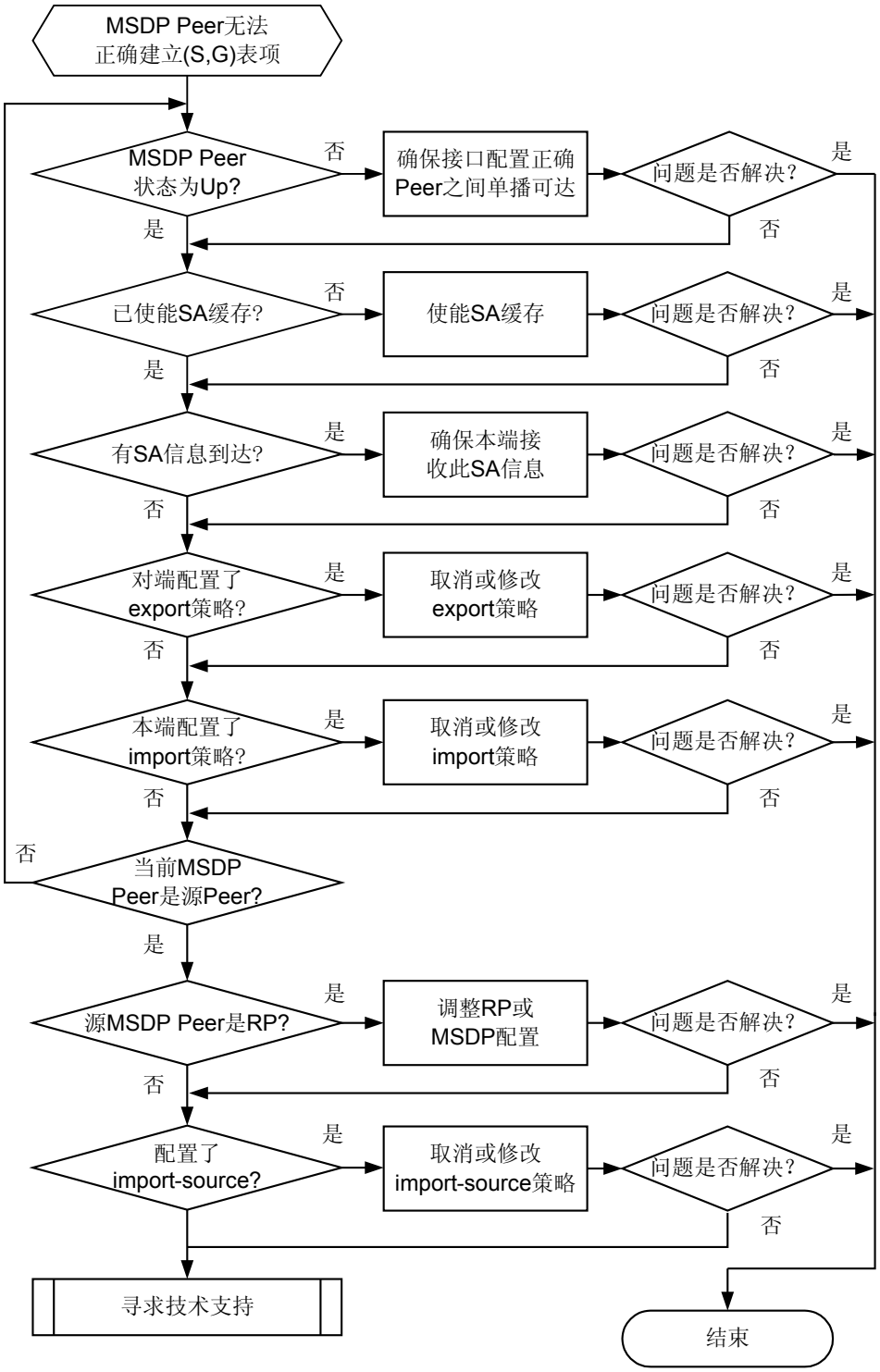
故障诊断流程

在配置组播网络后发现 MSDP 对等体无法正确建立（S,G）表项。

可按照故障诊断流程图 **8-5** 排除故障。

版权所有 © 华为技术有限公司

图 8-5 MSDP 对等体无法正确建立（S,G）表项故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查 MSDP 对等体状态是否为 Up

在配置了 MSDP 对等体的设备上执行 **display msdp brief** 命令，查看 MSDP 对等体状态是否为 Up。

- 如果显示信息表明 MSDP 对等体状态为 Down，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 不通问题**。
- 如果 MSDP 对等体都为 Up 状态，请执行**步骤 2**。

步骤 2 检查是否使能 SA 缓存

在 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看当前配置信息。

- 如果显示信息中出现“undo cache-sa-enable”，表明 MSDP 关闭了 SA 缓存。请在 MSDP 视图下执行 **cache-sa-enable** 命令使能 SA 缓存。
- 如果已经使能 SA 缓存，请执行**步骤 3**。

步骤 3 检查是否有对等体发出的 SA 信息到达

在 MSDP 对等体上执行 **display msdp sa-count** 命令，查看本设备上是否有 SA 缓存。

- 如果没有输出显示信息，请联系华为技术工程师。
- 如果显示信息中“Number of source”和“Number of group”不为 0，则说明收到了对等体发送的 SA 消息，请执行**步骤 4**。

步骤 4 检查 MSDP 对等体是否配置了 export 策略

在 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看当前配置信息。

- 如果 MSDP 对等体配置了 export 策略：
  - 如果显示信息中出现不带参数的“peer peer-address sa-policy export”，则表明该 MSDP 对等体不向外转发任何组播源信息，需要执行 **undo peer** *peer-address* **sa-policy export** 命令删除该配置。
  - 如果显示信息中出现带 ACL 参数的“peer peer-address sa-policy export acl advanced-acl-number”，则表明只有 ACL 允许的（S,G）表项才能被通告。查看设备上是否配置了相应的 ACL 命令，且（S,G）表项能否通过相应的 ACL 规则的过滤。请使用 **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 MSDP 对等体没有配置 export 策略，请执行**步骤 5**。

步骤 5 检查本端是否配置了 import 策略

在 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看当前配置。

- 如果 MSDP 对等体配置了 import 策略：
  - 如果显示信息中出现不带参数的“peer peer-address sa-policy import”，则表明该 MSDP 对等体不接收任何组播源信息，需要执行 **undo peer** *peer-address* **sa-policy import** 命令删除该配置。
  - 如果显示信息中出现带 ACL 参数的“peer peer-address sa-policy import acl advanced-acl-number”，则表明只有 ACL 允许的（S,G）表项才能被接收。查看设备上是否配置了相应的 ACL 命令，且（S,G）表项能否通过相应的 ACL 规则

版权所有 © 华为技术有限公司

的过滤。请使用 **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 MSDP 对等体没有配置 import 策略，请执行**步骤 6**。

步骤 6 检查当前 MSDP 对等体是否是源 MSDP 对等体

- 如果当前 MSDP 对等体不是源 MSDP 对等体，请在上游设备上按故障处理步骤进行排查。
- 如果当前 MSDP 对等体是源 MSDP 对等体，请执行**步骤 7**。

步骤 7 检查源 MSDP 对等体是否是 RP

在离组播源最近的 MSDP 对等体上执行 **display pim routing-table** 命令，查看路由表信息。

- 如果（S,G）表项上没有 2MSDP 标志，则表明该 MSDP 对等体不是 RP。调整 PIM-SM 网络 RP 或 MSDP 对等体的配置，确保源 MSDP 对等体为 RP。
- 如果源 MSDP 对等体配置为 RP，请执行**步骤 8**。

步骤 8 检查源 MSDP 对等体是否配置了 import-source 策略

通过执行 **import-source** [**acl** *acl-number*]命令，MSDP 可以在创建 SA 消息时，对其通告的（S,G）表项的组播源进行过滤，从而实现在创建 SA 消息时对组播源消息传播的控制。缺省情况下，SA 消息通告所有已知组播源信息。

在离组播源最近的 MSDP 对等体的 MSDP 视图下执行 **display this** 命令，查看的当前配置。

- 如果 MSDP 对等体配置了 import-source 策略：
  - 如果显示信息中出现不带参数的“import-source”，则表明该 MSDP 对等体不向外通告任何组播源信息，需要执行 **undo import-source** 命令删除该配置。
  - 如果显示信息中出现带 ACL 参数的“import-source acl acl-number”，则表明只有 ACL 允许的（S,G）信息才能被通告。查看设备是否配置了相应的 ACL 命令，且（S,G）表项能否通过相应的 ACL 规则的过滤。请执行 **undo import-source** 命令删除该配置或者调整指定的 ACL 规则。
- 如果 MSDP 对等体未配置 import-source 策略，请执行**步骤 9**。

步骤 9 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

8.1.6 组播设备无法正常建立 IGMP 表项的定位思路

常见原因

本类故障的常见原因主要包括：

- 设备没有使能组播
- 接口没有使能 IGMP，或者配置的 IGMP 版本不正确
- 接口收到的是 SSM 组地址范围的 EXCLUDE 报文
- 接口配置了组播边界或 Group-policy
- 接口配置了 IGMP 组成员关系的最大个数限制

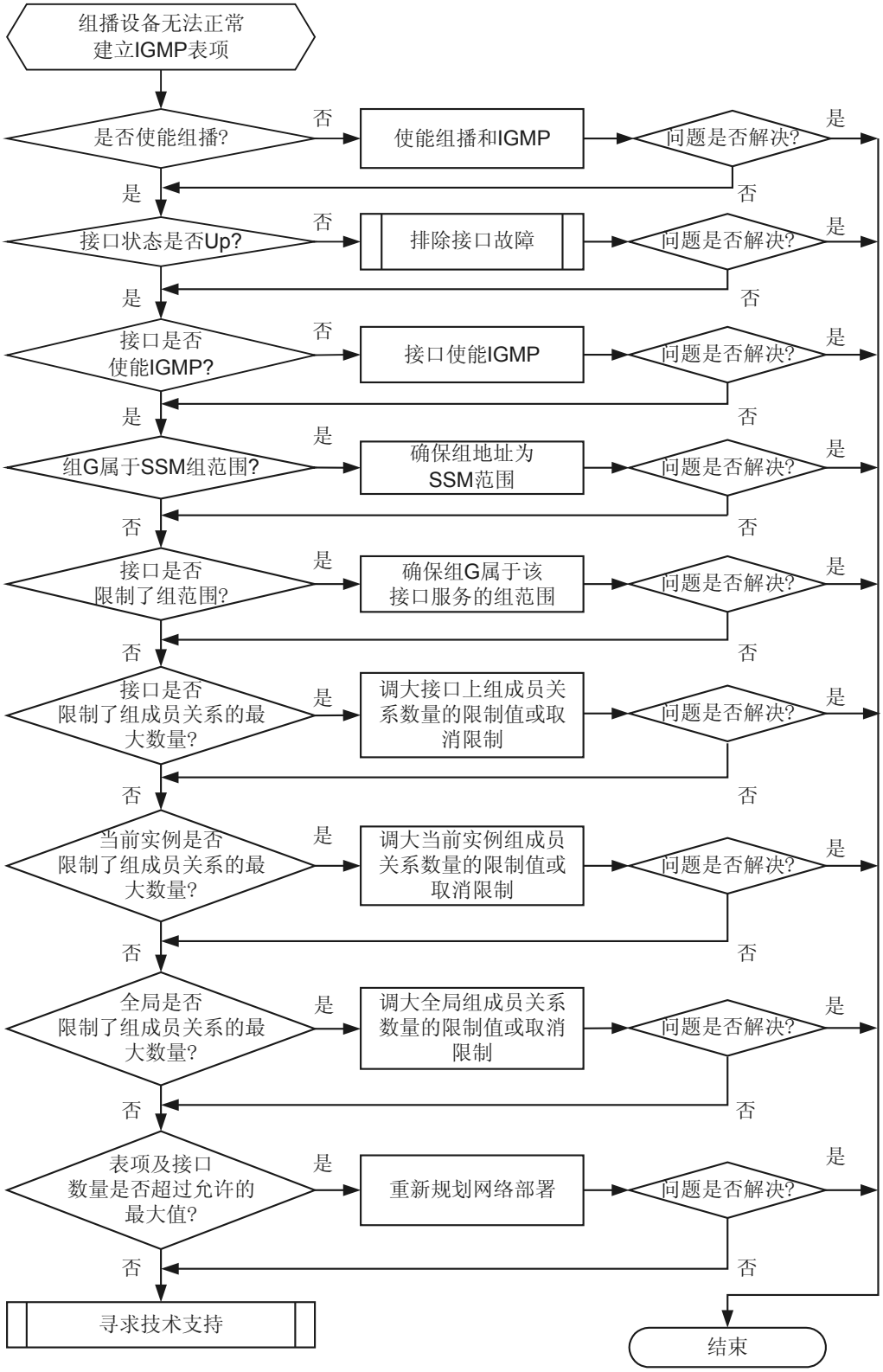
故障诊断流程

在配置组播网络后发现设备无法正常建立 IGMP 表项。

可按照故障诊断流程图 8-6 排除故障。

版权所有 © 华为技术有限公司

图 8-6 组播设备无法正常建立 IGMP 表项故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查设备是否使能组播

在直连用户主机网段的设备上执行 **display current-configuration** 命令，查看当前配置信息。

- 如果显示信息中没有“multicast routing-enable”，请首先在系统视图下执行 **multicast routing-enable** 命令使能组播功能，然后补充其他的 IGMP 相关配置。详细的配置方法请参见《Huawei AR2200-S 系列企业路由器 配置指南-组播》。
- 如果设备已经使能组播，请执行步骤 2。

步骤 2 检查接口是否为 Up 状态

在设备上执行 **display interface** *interface-type interface-number* 命令，指定该设备上与用户主机网段直连的接口，查看接口的显示信息。

- 如果显示信息为“current state : DOWN”，说明接口物理状态为 Down。请校正组网及接口接线。
- 如果显示信息为“Line protocol current state : DOWN”，说明接口的协议状态为 Down，则执行如下检查：
  - 检查该接口是否处于 Shutdown 状态。

    执行 **display current-configuration interface** *interface-type interface-number* 命令，查看接口上的当前配置。若显示信息中出现“shutdown”，请在接口视图下使用 **undo shutdown** 命令，取消此配置。
  - 检查该接口是否配置 IP 地址。

    执行 **display current-configuration interface** *interface-type interface-number* 命令查看接口地址。如果发现接口未配置 IP 地址或地址与主机不在同一网段，请使用 **ip address** *ip-address* { *mask* | *mask-length* }命令为接口配置 IP 地址。
- 如果接口为 Up 状态，请执行步骤 3。

步骤 3 检查接口是否使能 IGMP

在设备上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看直连客户端的接口的当前配置。

- 如果显示信息中没有“igmp enable”，说明未使能 IGMP。请在接口视图下执行 **igmp enable** 命令，使能 IGMP。
- 如果接口已经使能 IGMP，请执行步骤 4。

步骤 4 检查组播组 G 是否属于 SSM 组地址范围

在直连用户主机网段的设备上执行 **display current-configuration configuration pim** 命令，查看 PIM 视图下的当前配置信息。如果显示信息中出现“ssm-policy basic-acl-number”或“ssm-policy basic-acl-name”，则表明在该设备上指定了 SSM 组地址范围。执行 **display acl** { *acl-number* | **name** *acl-name* }命令，查看该 ACL 的配置信息。

- 如果显示信息表明 ACL 允许的组范围包括该组播组 G，则说明组播组 G 属于 SSM 组范围。则确保用户主机和设备接口之间运行 IGMPv3 版本。

版权所有 © 华为技术有限公司

如果主机上运行的 IGMP 版本无法升级，则需要在设备的接口上使能 SSM Mapping 功能，并设置与组播组 G 相关的 SSM 静态映射规则。

- 如果显示信息表明 ACL 允许的组范围不包括组播组 G，则说明组播组 G 属于 ASM 组范围，需要调整相应的 ACL 指定的组地址范围，使组播组 G 在该 ACL 的允许范围内。
- 如果组播组 G 是否属于 SSM 组地址范围且 IGMP 版本配置正确，请执行**步骤 5**。

步骤 5 检查接口上是否配置了限制用户加入的组范围

在设备上执行 **display igmp interface** *interface-type interface-number* 命令，查看直连客户端的接口上的当前配置。

- 如果显示信息中“group-policy”字段内容不是“none”，表明在该接口上限制了用户能够加入的组范围，IGMP 将按照指定的 ACL 过滤组成员加入信息。检查该 ACL 的所允许的组范围，如果组播组 G 在 ACL 允许范围外，请修改 ACL，或删除该配置，确保 IGMP 为组播组 G 的组成员服务。
- 如果接口没有配置限制用户加入的组范围，请执行**步骤 6**。

步骤 6 检查接口是否配置了限制 IGMP 组成员关系的最大数量

在设备上执行 **display igmp interface** *interface-type interface-number* 命令，查看直连客户端的接口上的当前配置。

- 如果显示信息中“IGMP limit”字段内容不是“-”，表明在该接口上配置了限制 IGMP 组成员关系的最大数量。在接口视图下执行 **igmp limit** *number* 命令将限制值调大，或使用 **undo igmp limit** 命令删除配置的限制值。
- 如果显示信息中“IGMP limit”字段内容是“-”，请执行**步骤 7**。

步骤 7 检查当前实例是否配置了限制 IGMP 组成员关系的最大数量

在设备上执行 **display current-configuration configuration igmp** 命令，查看相应实例配置的限制值。

- 如果显示信息中包含相应实例的 Limit 值，表明相应实例配置了限制 IGMP 组成员关系的最大数量。在相应实例的 IGMP 视图下执行 **limit** *number* 命令将限制值调大，或使用 **undo limit** 命令删除配置的限制值。
- 如果显示信息中不包含相应实例的 Limit 值，请执行**步骤 8**。

步骤 8 检查全局是否配置了限制 IGMP 组成员关系的最大数量

在设备上执行 **display current-configuration | include igmp global limit** 命令，查看全局配置值。

- 如果存在显示信息，表明全局配置了限制 IGMP 组成员关系的最大数量。在系统视图下执行 **igmp global limit** *number* 命令将限制值调大，或使用 **undo igmp global limit** 命令删除配置的限制值。
- 如果不存在显示信息，请执行**步骤 9**。

步骤 9 检查表项及接口数量是否超过产品允许的最大值

- 如果表项及接口数量超过产品允许的最大值，请重新规划网络部署。
- 如果检查结束，故障仍然无法排除，请执行**步骤 10**。

步骤 10 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

版权所有 © 华为技术有限公司

- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

9 QoS 类

关于本章

9.1 流策略故障处理
介绍流策略故障的定位思路和典型案例。

9.2 优先级映射故障处理

9.3 流量监管故障处理
介绍流量监管相关故障的定位思路和典型案例。

9.4 流量整形故障处理
介绍流量整形相关故障的定位思路和典型案例。

9.5 拥塞避免故障处理
介绍拥塞避免相关故障的定位思路和典型案例。

9.6 拥塞管理故障处理
介绍拥塞管理相关故障的定位思路和典型案例。

版权所有 © 华为技术有限公司

9.1 流策略故障处理

介绍流策略故障的定位思路和典型案例。

9.1.1 流策略不生效的定位思路

介绍流策略不生效的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

流策略不生效的常见原因包括：

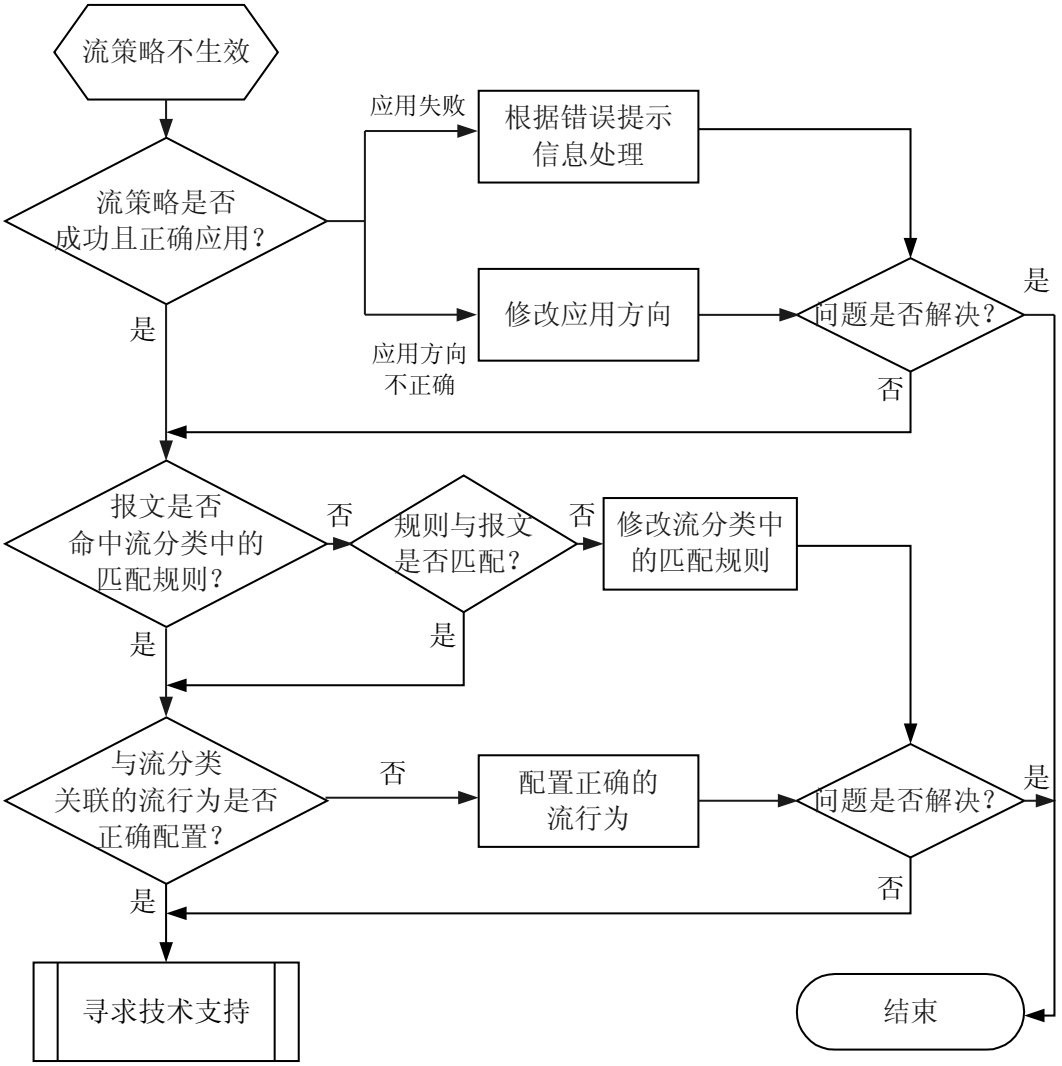
- 流策略应用失败。
- 流策略应用方向与业务需求不一致。
- 流策略中流分类的匹配规则与报文不匹配。
- 流策略中与流分类关联的流行为配置不正确。

故障诊断流程

可按照图 9-1 排除流策略不生效故障。

版权所有 © 华为技术有限公司

图 9-1 流策略不生效故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查流策略是否成功且正确应用

执行命令 **display traffic-policy applied-record**，查看当前流策略的应用记录：

- 如果显式信息中 Policy total applied times 字段为 0，表明该策略没有被应用，请在接口或子接口下执行命令 **traffic-policy** 正确应用流策略。
- 如果显示信息中 state 字段为 success，再检查流策略应用方向是否正确（对进入 AR2200-S 的报文实施策略时，流策略应用方向应为 inbound；对从 AR2200-S 发出的报文实施策略时，应用方向应为 outbound）：

版权所有 © 华为技术有限公司

- 如果流策略的应用方向不正确，则先执行命令 **undo traffic-policy** { **inbound** | **outbound** }取消错误的流策略应用，再执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }重新将流策略正确应用。
- 如果流策略的应用方向正确，请执行步骤 2。

● 如果流策略应用 **fail**，表明该流策略应用失败。流策略应用失败时，系统都会有错误提示信息，如果没有注意到，请在相应接口下先执行命令 **undo traffic-policy** { **inbound** | **outbound** }取消应用流策略，再执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }重新应用流策略，系统就会有错误提示信息，然后根据错误提示信息修复故障。

步骤 2 检查报文是否命中流分类中的匹配规则

执行命令 **display traffic policy statistics**，查看接口基于流策略的流量统计信息。如果显示信息中的各字段对应的内容为空，则报文没有命中流分类中的匹配规则；否则，报文命中流分类中的匹配规则。

说明

查看流量统计信息前，需要在流行为中使用命令 **statistic enable** 配置流量统计功能。

● 如果报文命中了流分类规则，执行步骤 4。
● 如果报文没有命中流分类规则，执行步骤 3。

步骤 3 检查报文特征是否与流分类规则匹配

根据故障现象判断报文特征（如 IP 地址、MAC 地址、DSCP 值、VLAN ID、802.1p 值等），然后执行命令 **display traffic policy user-defined** 查看流策略中绑定的流分类，再执行命令 **display traffic classifier user-defined** 查看流分类中的匹配规则。对比报文特征与流分类中的匹配规则，判断两者是否匹配：

● 如果报文特征与流分类中的规则不匹配，修改流分类规则，使之与报文特征匹配。
● 如果报文特征与流分类中的规则匹配，执行步骤 4。

步骤 4 检查流分类关联的流行为是否正确配置

执行命令 **display traffic-policy user-defined** *policy-name* **classifier** *classifier-name* 检查流分类关联的流行为是否符合业务需求。

● 如果不符合业务需求，则执行命令 **traffic behavior** 进入流行为视图，并配置正确的流行为。
● 如果符合业务需求，执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

● 上述步骤的执行结果。
● 设备的配置文件、日志信息、告警信息。

----结束

相关告警和日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

9.2 优先级映射故障处理

9.2.1 报文未进入正确队列的定位思路

介绍报文未进入正确队列的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

报文未按优先级入队列包括如下几种现象：

- 不同优先级的报文都进入了同一个队列。
- 不同优先级的报文能够入不同的队列，但进入的队列有误。
- 同一优先级报文进入同一个队列，但进入的队列有误。
- 同一优先级的报文进入不同的队列。

本类故障的常见原因主要包括：

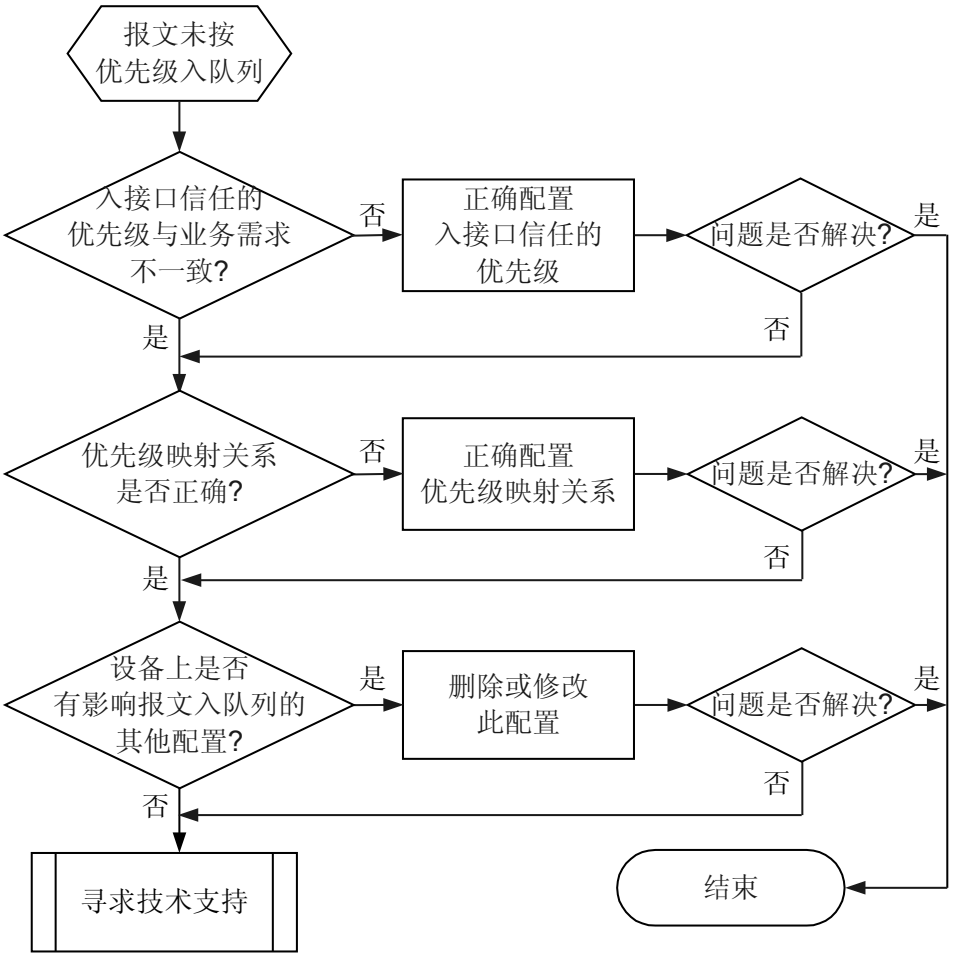
- 入接口信任的优先级与业务需求不一致。
- 优先级映射表中的与入队列有关的优先级映射关系与业务需求不一致（关注：DSCP、802.1p 或 EXP 到内部优先级之间的映射关系）。
- 设备上有影响报文入队列的配置，包括：
  - 报文入接口配置了带 **remark-8021p** 或 **remark-dscp** 参数的 **qos car inbound** 命令。
  - 报文入接口配置了 **traffic-policy inbound** 命令，且流策略里配置了 **remark 8021p**、**remark dscp**、**remark local-precedence** 等标记动作，或带 **remark-8021p**、**remark-dscp** 参数的 **car** 动作。
  - 报文出接口配置了 **traffic-policy outbound** 命令，且流策略里包含了 **queue af**、**queue ef** 或 **queue wfq** 等入队列动作。

故障诊断流程

如果报文未按优先级入队列，可按照图 9-2 所述流程排除故障。

版权所有 © 华为技术有限公司

图 9-2 报文未按优先级入队列的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查入接口信任的优先级是否符合业务需求

进入报文入接口视图，执行命令 **display this**，查看入接口配置的 **trust** 命令（如果不配置，系统缺省不信任任何优先级），看接口信任的优先级是否与业务需求一致：

说明

如果没有配置 **trust**，AR2200-S 按照 **port priority** 命令所配置的缺省 802.1p 优先级入队列，这将导致所有报文进入同一队列，无法提供差分服务。

- 如果接口信任的优先级与业务需求一致，执行命令 **trust** 修改入接口信任的优先级。
- 如果接口信任的优先级与业务需求一致，执行步骤 2。

步骤 2 检查优先级映射关系是否正确

版权所有 © 华为技术有限公司

AR2200-S 按照内部优先级入队列，因此，需要查看入接口所信任的报文优先级(如DSCP、8021p)到内部优先级的映射关系。

执行命令 **display qos map-table** 检查与报文优先级映射表中配置的优先级映射关系是否符合业务规划:

- 如果配置不符合业务规划，请执行命令 **qos map-table** 进入优先级映射表视图，然后执行命令 **input** 正确配置。
- 如果配置符合业务规划，请执行步骤 3。

步骤 3 检查报文入接口是否有影响报文入队列的其他配置

1. 检查报文入接口是否配置了带 remark 动作的流量监管

   进入入接口视图，执行命令 **display this**，查看接口上是否配置了带 **remark-8021p** 或 **remark-dscp** 参数的 **qos car inbound** 命令。

   - 如果配置了，请根据实际情况取消 reamrk 动作或执行命令 **undo qos car inbound** 取消配置的流量监管。
   - 如果没有配置，请执行步骤 b。

2. 检查报文入接口是否配置了带 remark 动作的入方向的流策略

   进入入接口视图，执行命令 **display this**，查看接口上是否配置了 **traffic-policy inbound** 命令。

   - 如果配置了，则请执行命令 **display traffic-policy applied-record** 查看流策略的应用记录及其绑定的流行为，如果流策略应用 **success**，请进一步执行命令 **display traffic behavior user-defined** 查看该流策略绑定的流行为里是否包含 remark 报文优先级（如 **remark 8021p**、**remark dscp**）或 **remark local-precedence** 的动作。
     - 如果流策略绑定的流行为中配置了相应的 remark 动作，请根据需要取消流行为中的 remark 动作或者取消接口上的流策略配置。
     - 如果流策略应用失败或者流策略绑定的流行为中没有配置 remark 动作，请执行步骤 c。
   - 如果没有配置，请执行步骤 c。

3. 检查报文出接口是否配置了带入队列动作的出方向的流策略

   进入入接口视图，执行命令 **display this**，查看接口上是否配置了 **traffic-policy outbound** 命令。

   - 如果配置了，请执行命令 **display traffic-policy applied-record** 查看流策略的应用记录及其绑定的流行为，如果流策略应用 **success**，请进一步执行命令 **display traffic behavior user-defined** 查看该流策略绑定的流行为的配置信息。
     - 如果流策略绑定的流行为的配置信息中包含 **Assured Forwarding**、**Expedited Forwarding** 或 **Flow based Weighted Fair Queueing** 等关键字时，表明该流行为中有入队列的动作，请根据需要取消流行为中的入队列动作或者取消接口上的流策略配置。
     - 如果流策略应用失败或者流策略绑定的流行为中配置入队列动作，请执行步骤 4。
   - 如果没有配置，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

版权所有 © 华为技术有限公司

- 设备的配置文件、日志信息、告警信息。

----结束

相关告警和日志

相关告警

无

相关日志

无

9.2.2 优先级映射结果不正确的定位思路

介绍优先级映射结果不正确的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

优先级映射结果不正确的

常见原因

优先级映射结果不正确的常见原因主要包括：

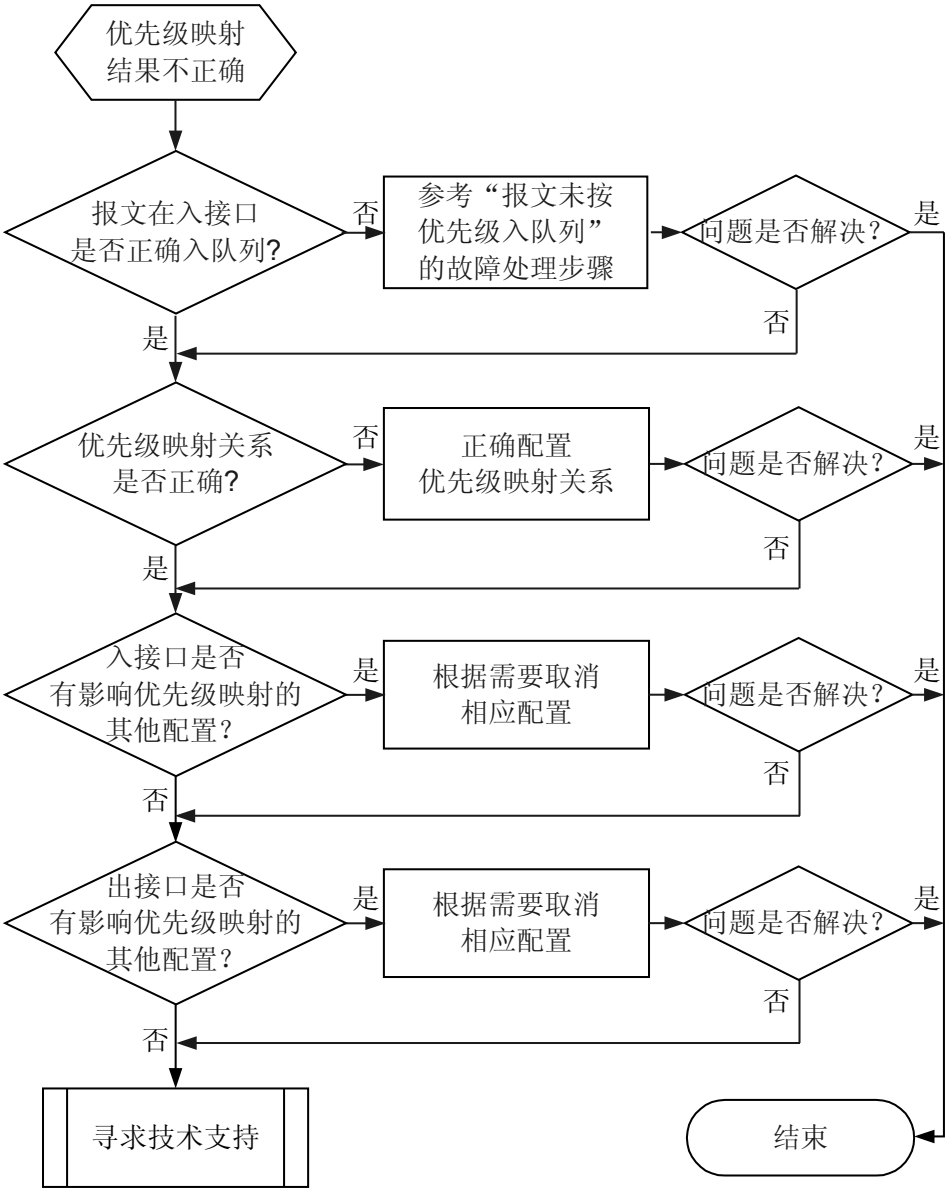
- 报文没有携带报文入接口信任的优先级。
- 报文入接口配置的 **trust** 没有带 **override** 属性。
- 优先级映射表中配置的优先级映射关系与要求不一致。
- 报文入接口有影响优先级映射的配置，包括：
  - 配置了带 **remark-8021p** 或 **remark-dscp** 参数的 **qos car inbound** 命令。
  - 配置了带 **remark 8021p**、**remark dscp**、**remark local-precedence** 等标记动作，或带 **remark-8021p** 或 **remark-dscp** 参数的 **car** 动作的 **traffic-policy inbound** 命令。
- 报文出接口有影响优先级映射的配置，包括：
  - 配置了带 **remark-8021p** 或 **remark-dscp** 参数的 **qos car outbound** 命令。
  - 配置了带 **remark 8021p**、**remark dscp**、**remark local-precedence** 等标记动作，或带 **remark-8021p** 或 **remark-dscp** 参数的 **car** 动作的 **traffic-policy outbound** 命令。

故障诊断流程

如果从 AR2200-S 出去的报文优先级不正确，可按照**图 9-3** 排除故障。

版权所有 © 华为技术有限公司

图 9-3 优先级映射结果不正确故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查报文是否携带报文入接口信任的优先级

进入报文入接口视图，执行命令 **display this**，查看入接口配置的 **trust** 命令（如果不配置，AR2200-S 缺省不信任任何优先级），然后抓取入接口的报文，分析其携带的优先级，查看其是否为接口信任的优先级：

版权所有 © 华为技术有限公司

说明

如果配置了 **trust**，但报文没有携带入接口信任的优先级，此时若配置了 **override** 属性，AR2200-S 按照 **port priority** 命令所配置的缺省 802.1p 优先级查找 802.1p 优先级到各优先级映射表，修改报文的优先级。

- 如果报文没有携带入接口信任的优先级，执行命令 **trust** 修改入接口信任的优先级为报文携带的优先级。
- 如果报文携带了入接口信任的优先级，请执行步骤 2。
- 如果报文携带了入接口信任的优先级，请关注 **trust** 命令是否带了 **override** 属性：
  - 如果没有带 **override** 属性，则 AR2200-S 按照指定优先级映射后，并不修改报文的优先级，需要修改配置使带有 **override** 属性。
  - 如果已带 **override** 属性，请执行步骤 2。

步骤 2 检查优先级映射关系是否正确

执行命令 **display qos map-table** 检查接口所信任的优先级与所需优先级之间的优先级映射关系是否符合业务规划:

- 如果配置不符合业务规划，请执行命令 **qos map-table** 修改配置。
- 如果配置符合业务规划，请执行步骤 3。

步骤 3 检查报文入接口是否有影响优先级映射的其他配置

1. 检查报文入接口是否配置了带 **remark** 参数的基于接口的流量监管

   由于基于接口的流量监管的优先级高于优先级映射，如果入接口配置了带 **remark-8021p** 或 **remark-dscp** 参数的基于接口的流量监管，AR2200-S 按照流量监管中 **remark** 后的优先级标记报文。

   进入入接口视图，执行命令 **display this**，查看接口上是否配置了带 **remark-8021p** 或 **remark-dscp** 参数的 **qos car inbound** 命令。

   - 如果配置了，请根据实际情况取消 **reamrk** 动作或执行命令 **undo qos car inbound** 取消配置的流量监管。
   - 如果没有配置，请执行步骤 b。

2. 检查报文入接口是否配置了带 **remark** 动作的入方向的流策略

   由于流策略的优先级高于优先级映射，如果入接口配置了带 **remark** 报文优先级、**remark local-precedence**，或带 **remark-8021p** 或 **remark-dscp** 参数的 **car** 等动作的流策略，AR2200-S 按照流策略中 **remark** 后的优先级标记匹配流分类的报文。

   进入入接口视图，执行命令 **display this**，查看接口上是否配置了 **traffic-policy inbound** 命令。

   - 如果配置了，则请执行命令 **display traffic-policy applied-record**，查看流策略的应用记录及其绑定的流行为。

     如果流策略应用 **success**，请进一步执行命令 **display traffic behavior user-defined** 查看该流策略绑定的流行为里是否包含 **remark** 报文优先级、**remark** 内部优先级，或者带 **remark-8021p** 或 **remark-dscp** 参数的 **car** 等动作。
     - 如果流策略绑定的流行为中配置了上述动作，请根据需要取消流行为中的相应动作或者取消接口上的流策略配置。
     - 如果流策略应用 **fail** 或者流策略绑定的流行为中没有配置上述动作，请执行步骤 c。
   - 如果没有配置，请执行步骤 c。

版权所有 © 华为技术有限公司

步骤 4 检查报文出接口是否有影响优先级映射的其他配置

1. 检查报文出接口是否配置了带 **remark** 参数的基于接口的流量监管

   由于基于接口的流量监管的优先级高于优先级映射，如果出接口配置了带 **remark-8021p** 或 **remark-dscp** 参数的基于接口的流量监管，AR2200-S 按照流量监管中 **remark** 后的优先级标记报文。

   进入入接口视图，执行命令 **display this**，查看接口上是否配置了带 **remark-8021p** 或 **remark-dscp** 参数的 **qos car outbound** 命令。

   - 如果配置了，请根据实际情况取消 **reamrk** 动作或执行命令 **undo qos car outbound** 取消配置的流量监管。
   - 如果没有配置，请执行步骤 b。

2. 检查报文出接口是否配置了带 **remark** 动作的出方向的流策略

   由于流策略的优先级高于优先级映射，如果出接口配置了带 **remark** 报文优先级、**remark local-precedence**，或带 **remark-8021p** 或 **remark-dscp** 参数的 **car** 等动作的流策略，AR2200-S 按照流策略中 **remark** 后的优先级标记匹配流分类的报文。

   进入出接口视图，执行命令 **display this**，查看接口上是否配置了 **traffic-policy outbound** 命令。

   - 如果配置了，则请执行命令 **display traffic-policy applied-record** 查看流策略的应用记录及其绑定的流行为。

     如果流策略应用 **success**，请进一步执行命令 **display traffic behavior user-defined**，查看该流策略绑定的流行为里是否包含 **remark** 报文优先级、**remark** 内部优先级，或者带 **remark-8021p** 或 **remark-dscp** 参数的 **car** 等动作。

     - 如果流策略绑定的流行为中配置了上述动作，请根据需要取消流行为中的该动作或者取消接口上的流策略配置。
     - 如果流策略应用 **fail** 或者流策略绑定的流行为中没有配置上述动作，请执行步骤 5。
   - 如果没有配置，请执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警和日志

相关告警

无

相关日志

无

9.2.3 故障处理案例

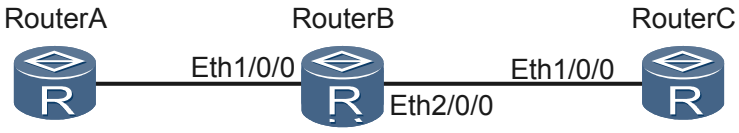
介绍优先级映射相关的典型故障案例。

版权所有 © 华为技术有限公司

报文未进入正确队列

网络环境

图 9-4 报文未进入正确队列组网图



在如图 9-4 所示组网中，RouterA 过来的报文带 VLAN 100，优先级为 0 ～ 7，在 RouterB 上执行命令 **display qos queue statistics** 查看出接口 Eth2/0/0 的流量统计时，发现报文未按照其优先级入队列，显示信息如下：

说明

只有在接口使用命令 **qos queue-profile** 应用队列模板后，才能使用命令 **display qos queue statistics** 查看到统计计数。

```
<RouterB> display qos queue statistics interface ethernet 2/0/0
```

Queue	Passed(Packets/Bytes)	Dropped(Packets/Bytes)
0	**116,975/0**	**0/0**
1	0/0	0/0
2	0/0	0/0
3	0/0	0/0
4	0/0	0/0
5	0/0	0/0
6	0/0	0/0
7	0/0	0/0

显示信息表明，报文没有按照报文的 802.1p 优先级入队列，而是都进入了队列 0。

故障分析

报文未按照其优先级进入相应的队列，一般是优先级与队列之间的映射出了问题。

1. 检查 RouterB 的入接口配置，看是否有影响报文入队列的配置。
   a. 在 RouterB 的入接口 Eth2/0/0 处执行命令 **display this**。

```
[RouterB-Ethernet2/0/0] display this
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

显示信息表明，入接口 Eth2/0/0 上仅配置允许 VLAN 100 报文通过，不会影响报文入队列，但接口没有配置信任 802.1p 优先级。

版权所有 © 华为技术有限公司

AR2200-S 中，如果报文入接口没有配置信任报文优先级，缺省不信任任何优先级。此时，AR2200-S 根据接口缺省 802.1p 优先级查找 802.1p 优先级到内部优先级的映射表，并根据映射后的内部优先级将报文入队列。

接口上没有配置 **port priority**，使用缺省值。缺省情况下，接口的缺省 802.1p 优先级值为 0。因此，所有的报文均进入 0 队列。

2. 查看 802.1p 优先级到内部优先级的映射关系。

执行命令 **display qos map-table dot1p-lp**

```
<RouterB> display qos map-table dot1p-lp
Input Dot1p      LP
-------------------
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
```

显示信息表明，对应 802.1p 优先级 0 的内部优先级也为 0。因此，所有报文均进入 0 号队列。

操作步骤

步骤 1 在 RouterB 上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface ethernet** 2/0/0，进入报文入接口视图。

步骤 3 执行命令 **trust 8021p**，配置接口信任 802.1p 优先级。

完成上述操作后，执行命令 **display qos queue statistics interface ethernet** 2/0/0 查看报文出接口的报文统计信息，看到 802.1p 优先级为 0 ～ 7 的报文均能够按其优先级入队列。故障排除。

----结束

案例总结

缺省情况下，AR2200-S 不信任报文的优先级，如果需要按报文优先级入队列，需要在报文入接口配置信任报文优先级。

由于未配置信任优先级导致优先级映射不正确

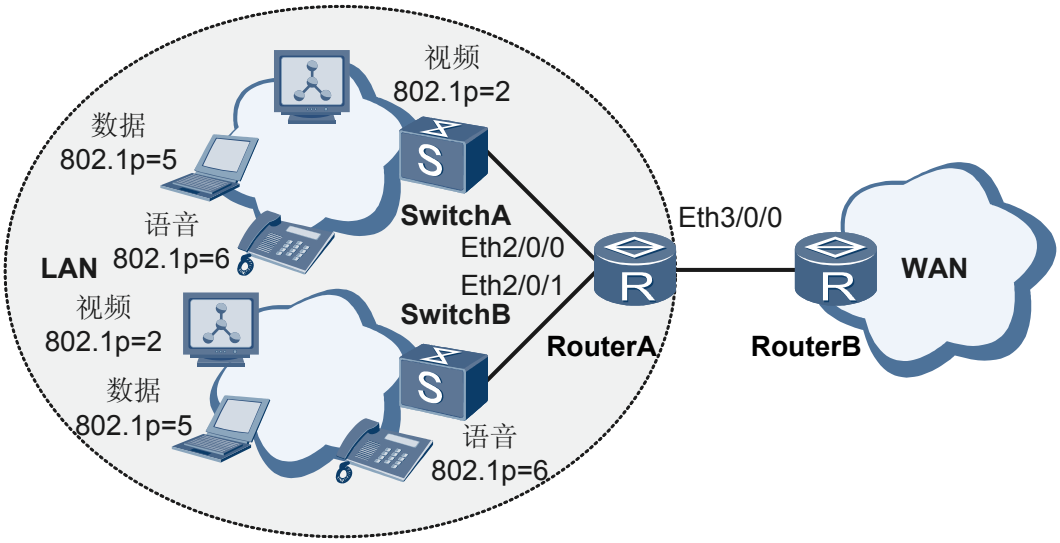
网络环境

在如图 9-5 所示组网中，企业网内部 LAN 侧的语音、视频和数据业务通过 SwitchA 和 SwitchB 连接到 RouterA 的 Eth2/0/1 和 Eth2/0/0 上，并通过 RouterA 的 GE3/0/0 接口连接到 WAN 侧网络。

不同业务的报文在 LAN 侧使用 802.1p 优先级进行标识，在 RouterA 上根据报文的 802.1p 优先级入队列，当报文从 GE3/0/0 接口到达 WAN 侧时，需要根据报文的 DSCP 优先级提供差分服务。因此，在 Router 上配置优先级映射。

版权所有 © 华为技术有限公司

图 9-5 由于未配置信任优先级导致优先级映射不正确组网图



配置后，发现 RouterB 上接收到的语音、视频和数据业务流中的 DSCP 值相同。

故障分析

1. 抓取从 RouterA 的 GE3/0/0 接口出去的报文并分析，发现语音、视频和数据业务流携带的 DSCP 优先级均为 0。
2. 检查优先级映射关系是否正确

   执行命令 **display qos map-table dot1p-dscp**，查看 802.1p 优先级到 DSCP 优先级的映射关系。

```
<RouterA> display qos map-table dot1p-dscp
Input Dot1p      DSCP
------------------
0                0
1                8
2               16
3               24
4               32
5               40
6               48
7               56
```

   显示信息表明，802.1p 优先级 2、5、6 分别映射到 DSCP 优先级 16、40、48，映射关系没有问题。
3. 检查入接口信任的优先级是否正确。

   进入报文入接口视图，执行命令 **display this**，查看接口配置。

```
<RouterA> system-view
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] display this
#
trust 8021p
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] display this
#
trust 8021p
traffic-policy tp1 inbound
```

   显示信息表明，在 RouterA 的接口 Eth2/0/0 和 Eth2/0/1 上配置了信任 802.1p 优先级，但没有带 **override** 属性。

版权所有 © 华为技术有限公司

AR2200-S 上，配置接口信任某种优先级，报文按照指定优先级映射，然后根据是否指定 **override** 属性，决定是否修改报文的优先级。如果不指定 override 属性，则不修改报文优先级。本例中，**trust** 命令没有指定 **override** 属性，因此，报文的 DSCP 优先级不会修改，仍然为缺省值 0。

操作步骤

步骤 1 执行命令 **interface ethernet 2/0/1**，进入报文入接口 Eth2/0/1 视图。

步骤 2 执行命令 **trust 8021p override**，配置接口信任 802.1p 优先级，并指定 **override** 属性。

步骤 3 执行命令 **interface ethernet 2/0/0**，进入报文入接口 Eth2/0/0 视图。

步骤 4 执行命令 **trust 8021p override**，配置接口信任 802.1p 优先级，并指定 **override** 属性。

完成上述操作后，RouterB 上接收到的来自企业网内部的语音、视频和数据业务流中的 DSCP 值均不相同，且与配置一致，故障排除。

----结束

案例总结

AR2200-S 上，如果要按照报文携带的优先级进行优先级映射，须在报文入接口配置信任该报文优先级，且指定 **override** 属性，否则，报文的优先级不会修改。

9.3 流量监管故障处理

介绍流量监管相关故障的定位思路和典型案例。

9.3.1 基于类的流量监管不生效

介绍基于类的流量监管不生效故障的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

基于类的流量监管实质是对流实施动作为 CAR 或共享 CAR 的流策略，因此其故障定位思路与流策略的相同，请参见 **9.1.1 流策略不生效的定位思路**。

9.3.2 基于接口的流量监管限速不准确的定位思路

介绍基于接口的流量监管限速不准确的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

基于接口的流量监管限速不正确包括如下两种现象：

- 流量监管不生效。
- 流量监管限速结果不准（即与业务要求不一致）。

本类故障的常见原因主要包括：

- 接口上没有配置 **qos car**。
- 配置的方向或 CAR 参数不正确（与业务规划不符）。

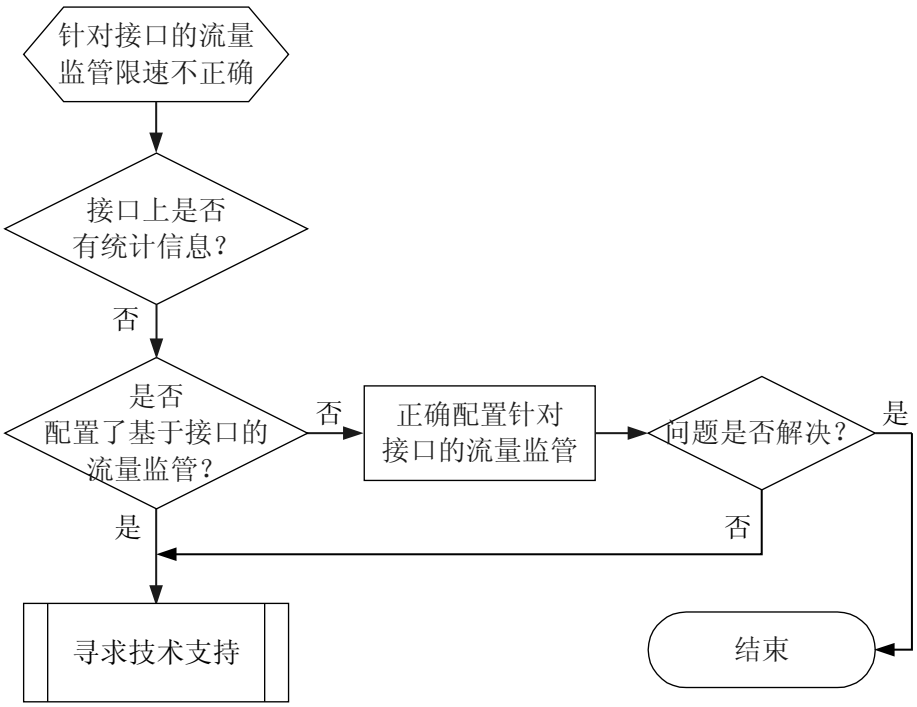
版权所有 © 华为技术有限公司

- 接口同时配置了与 **qos car** 方向相同的基于流的流量监管，且基于流的流量监管 CAR 值小于基于接口的流量监管 CAR 值。

故障诊断流程

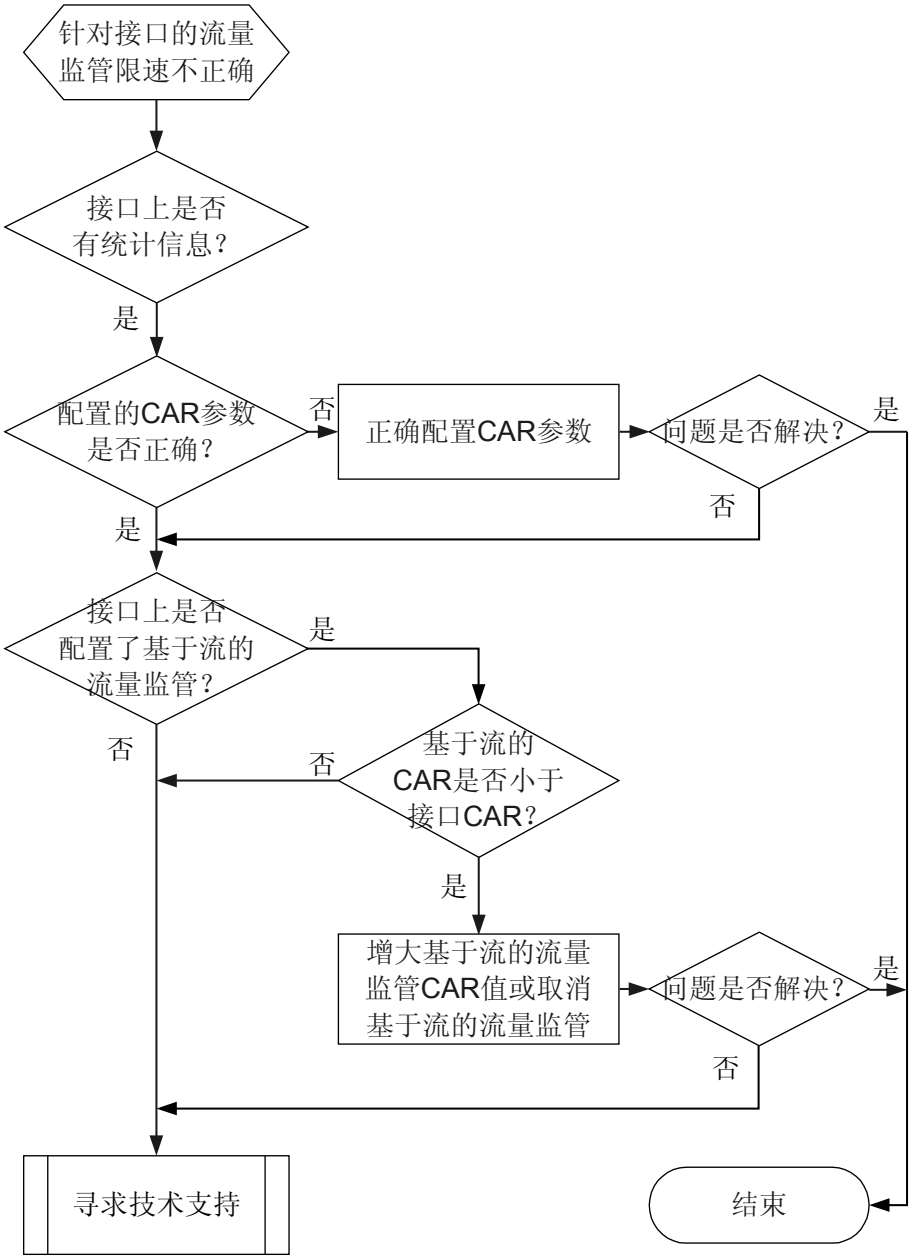
如果针对接口的流量监管限速不生效，请使用如图 9-6 所示的故障诊断流程处理；如果针对接口的流量监管限速不准，请使用如图 9-7 所示的故障诊断流程处理。

图 9-6 基于接口的流量监管不生效的故障诊断流程图



版权所有 © 华为技术有限公司

图 9-7 基于接口的流量监管限速不准的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查应用了基于接口的流量监管后的报文统计信息

执行命令 **display qos car statistics**，查看接口上通过和丢弃的报文统计信息。

版权所有 © 华为技术有限公司

- 如果没有任何显示信息，表明接口上没有配置基于接口的流量监管或者基于接口的流量监管不生效，请执行步骤 2。
- 如果有显示信息，表明基于接口的流量监管已配置成功，请执行步骤 3。

步骤 2 检查接口上是否正确配置了基于接口的流量监管。

进入接口视图，执行命令 **display this**，检查接口是否配置了命令 **qos car**。

- 如果没有配置，请执行命令 **qos car** 正确配置。
- 如果已经配置，请检查配置的方向是否正确（限制进入接口的流量速率，需使用 **inbound** 参数；限制流出接口的流量速率，需使用 **outbound** 参数）：

  说明

  AR2200-S 上，LAN 侧单板仅支持入方向的基于接口的流量监管。

  - 如果配置的方向不正确，请执行命令 **qos car** 正确配置。
  - 如果配置的方向正确，请执行步骤 3。

步骤 3 检查配置的 CAR 参数是否正确

查看配置的 **qos car** 中的 CIR 值，看其在粒度允许的误差范围内，是否能满足业务规划要求。

说明

还需要注意 CBS 的取值，如果 CBS 取值较大，会造成流量监管生效较慢，耗时较长，此时可等待一段时间或减少 CBS 值后再观察流量监管是否生效。

- 如果 CAR 参数不正确，请执行命令 **qos car** 修改 CAR 参数。
- 如果 CAR 参数正确，请执行步骤 4。

步骤 4 检查接口上是否同时配置了基于流的流量监管。

说明

如果接口上同时配置了方向相同的基于接口的流量监管和基于流的流量监管，系统按照 CAR 值小的限速。

进入接口视图，执行命令 **display this**，检查接口是否配置了方向与 **qos car** 相同的 **traffic-policy** 命令。

- 如果配置了，请执行命令 **display traffic-policy applied-record** 查看流策略的应用记录及其绑定的流行为，如果流策略应用 **success**，请进一步执行命令 **display traffic behavior user-defined** 查看该流策略绑定的流行为的配置信息。
  - 如果流行为配置信息中包含 CAR，且其值小于基于接口的流量监管 CAR 值，系统按照该流行为中的 CAR 值限速，请根据需要增加流行为中的 CAR 值或者取消接口上的流策略配置。
  - 如果流策略应用 **fail**、流策略绑定的流行为中配置的不是 CAR 或者流行为中的 CAR 值大于基于接口的流量监管 CAR 值，请执行步骤 5。
- 如果没有配置，请执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警和日志

相关告警

无

相关日志

无

9.3.3 故障处理案例

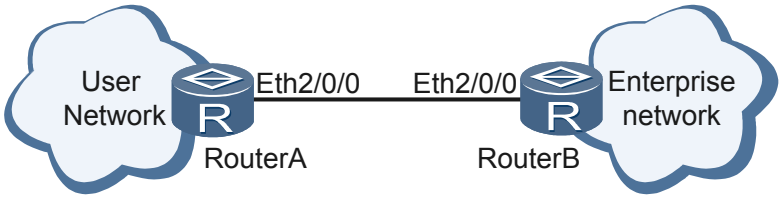
介绍基于接口的流量监管相关的典型故障案例。

基于接口的流量监管不生效

网络环境

如图 9-8 所示，为保护企业网网络，在 RouterA 接口 Eth2/0/0 上配置流量监管，限制 RouterA 上行流量速率为 10Mbit/s。但是当从用户网络往 RouterA 发送速率为 20Mbit/s 的流量时，发现从 RouterA 发出去的流量速率仍然为 20Mbit/s，流量监管功能没有生效。

图 9-8 基于接口的流量监管不生效组网图



故障分析

1. 检查报文在 RouterA 的出接口上是否配置了出方向的流量监管。

   进入 RouterA 上的接口 Eth2/0/0 视图，然后执行命令 **display this**，检查接口是否配置了出方向的流量监管。

```
[RouterA-Ethernet2/0/0] display this
[V200R001C00B130]
#
interface Ethernet2/0/0
 ip address 10.0.0.1 255.255.255.0
 qos car inbound cir 10000 cbs 1880000 pbs 3130000 green pass yellow pass red discard
#
return
```

   显示信息表明，接口 Eth2/0/0 上配置了 **inbound** 方向的流量监管，此配置仅对进入该接口的流量进行限速，对出方向流量不生效。

操作步骤

步骤 1 在 RouterA 上执行命令，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **interface ethernet 2/0/0**，进入接口 Eth2/0/0 视图。

步骤 3 执行命令 **qos car outbound cir 10000**，配置出方向的流量监管，限制出口流量速率为 10Mbps。

完成上述操作后，向 RouterA 发送速率为 20Mbps 的流量，查看从接口 Eth2/0/0 发送出去的流量，发现其速率为 10Mbps，流量监管生效，故障排除。

----结束

案例总结

如果基于接口的流量监管不生效，需要查看接口上是否配置了相应流向的基于接口的流量监管。其中：若配置有 **qos car inbound**，流量监管对进入接口的流量生效；若配置有 **qos car outbound**，流量监管对从接口出去的流量生效。

9.4 流量整形故障处理

介绍流量整形相关故障的定位思路和典型案例。

9.4.1 基于队列的流量整形结果不正确的定位思路

介绍基于队列的流量整形结果不正确的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

队列流量整形结果不正确的常见原因包括：

- 没有配置正确的队列整形参数。
- 基于接口的流量整形 CIR 小于接口上所有队列的流量整形 CIR 之和，致使队列流量整形带宽得不到保证。
- 因配置错误（如优先级映射关系与业务需求不一致等）导致报文没有进入配置了整形的队列。
- 各队列采用混合调度模式，且有大量报文进入 PQ 队列，致使其他队列流量整形带宽得不到保证。

  说明

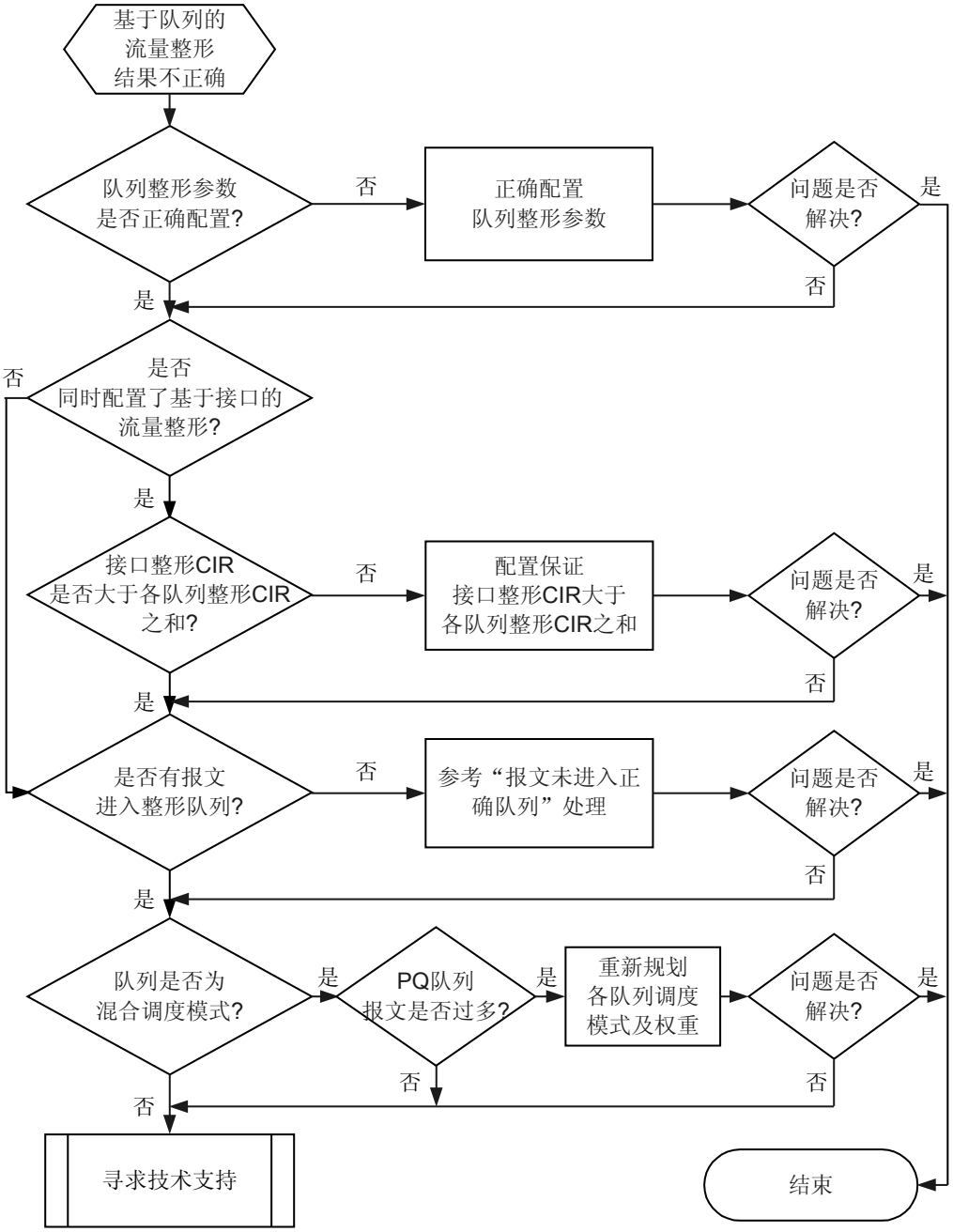
  混合调度模式下，队列的流量整形 CIR 没有得到满足在带宽不足的情况下是正常现象。

故障诊断流程

如果基于队列的流量整形结果不正确，请使用如图 9-9 所示的故障诊断流程处理。

版权所有 © 华为技术有限公司

图 9-9 基于队列的流量整形结果不正确的故障诊断流程图



故障处理步骤

说明

请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。

协议报文的优先级最高，如果有协议报文进入队列，会抢占队列带宽，造成短暂的整形不准确。此时，可等待一段时间再观察流量整形结果。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查接口上是否配置正确的队列整形参数

进入接口视图，使用命令 **display this**，检查接口上是否配置有 **qos queue-profile** 命令：

- 如果已配置，请执行命令 **display qos queue-profile** *queue-profile-name*，查看队列模板的配置信息。
  - 如果显示信息中各队列的 GTS(CIR/CBS)字段取值为缺省值“-/-”，表明队列模板中没有配置队列的流量整形，请进入队列模板视图，并执行命令 **queue gts** 正确配置队列的流量整形。
  - 如果显示信息中各队列的 GTS(CIR/CBS)字段取值不为缺省值，表明队列模板中已配置队列的流量整形，请记录配置流量整形的队列索引号，然后执行步骤 2。
- 如果没有配置，请执行命令 **qos queue-profile** 进行正确配置。

步骤 2 检查接口是否同时配置了基于接口的流量整形

查看接口下是否配置了 **qos gts** 命令：

- 如果配置了，请执行步骤 3。
- 如果没有配置，请执行步骤 4。

步骤 3 检查基于接口的流量整形 CIR 是否大于接口上所有队列的流量整形 CIR 之和

比较端口整形 CIR 与该端口上各队列整形 CIR 之和：

- 如果基于接口的流量整形 CIR 小于等于基于队列的流量整形 CIR 之和，则队列要求的带宽将得不到保证，会出现队列流量整形不准现象，请执行命令 **qos gts** 修改基于接口的流量整形参数，保证基于接口的流量整形 CIR 大于该接口上所有队列的流量整形 CIR 之和。
- 如果基于接口的流量整形 CIR 大于该接口上所有队列的流量整形 CIR 之和，则执行步骤 4。

步骤 4 检查是否有报文进入指定整形队列

执行命令 **display qos queue statistics interface** *interface-type interface-number*，检查接口上各队列的报文统计信息。

- 如果显示信息中对应配置流量整形的队列的 Passed 和 Dropped 字段取值分别为缺省值“0/0”，表明报文没有进入整形队列，请参见 **9.2.1 报文未进入正确队列的定位思路**进行故障定位。
- 如果显示信息中对应配置流量整形的队列的 Passed 和 Dropped 字段取值分别不为缺省值，表明有报文进入整形队列，请进一步观察是否有大量报文（如 GigabitEthernet 接口上报文速率超过 100Mbit/s，Ethernet 接口上报文速率超过 10Mbit/s）进入 PQ 队列：
  - 如果有大量报文进入 PQ 队列，请执行步骤 5。
  - 如果没有大量报文进入 PQ 队列，请执行步骤 6。

步骤 5 检查队列是否采用混合调度模式

进入接口视图，使用命令 **display this**，检查端口各队列调度模式：

- 如果各队列中既配置了 **schedule pq**，又配置了 **schedule wrr**、**schedule drr** 或 **schedule wfq**，则各队列是混合调度模式。

  混合调度模式下，当接口上有流量的时候，系统优先满足 PQ 队列的调度，然后再满足 WRR、DRR 或 WFQ 队列的 CIR，最后把剩余的带宽按照调度权重来进行分配。当 PQ 队列有大量报文时，会影响 WRR、DRR 或 WFQ 队列的流量整形效果。

版权所有 © 华为技术有限公司

请执行命令 **qos queue-profile** 命令进入队列模板视图，然后执行命令 **schedule** 和 **queue weight** 重新规划各队列的调度模式及权重，减少进入 PQ 队列的报文数。

说明

混合调度模式下，队列的流量整形 CIR 没有得到满足在带宽不足的情况下是正常现象。

- 如果各队列调度模式均为 **schedule pq**、**schedule wrr**、**schedule drr** 或 **schedule wfq**，则执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警和日志

相关告警

无

相关日志

无

9.4.2 故障处理案例

介绍流量整形相关的典型故障案例。

队列流量整形结果不正确

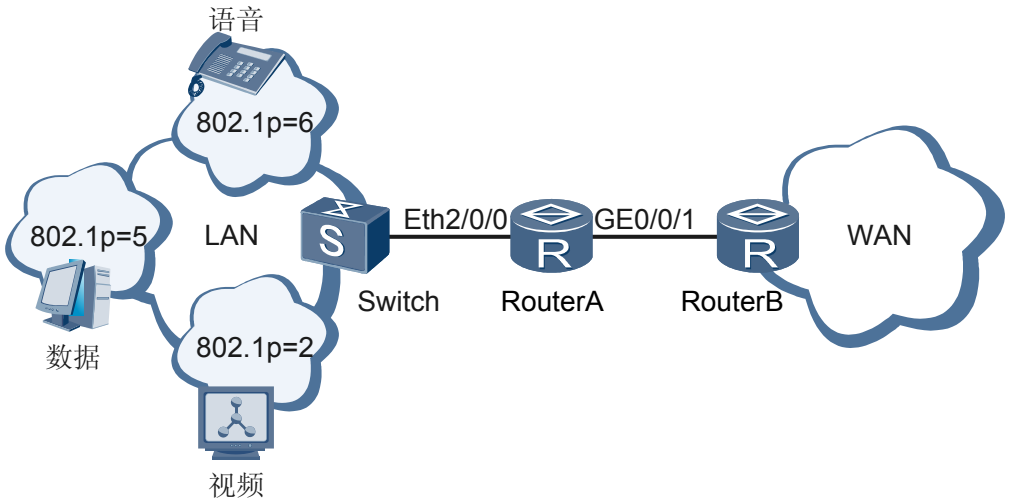
网络环境

在如图 9-10 所示组网中。由于来自 LAN 侧的流量速率大于 WAN 接口的速率，RouterA 的下行接口 GE0/0/1 处可能会发生带宽抖动。为减少带宽抖动，同时保证各类业务的带宽要求，在 RouterA 上配置使语音、视频、数据的业务流分别进入队列 6、2、5，并配置队列流量整形，使：

- 语音限速为 100kbps
- 视频限速为 2000kbps
- 数据限速为 500kbps

版权所有 © 华为技术有限公司

图 9-10 队列流量整形结果不正确配置组网图



配置后，发现语音、视频的带宽达不到要求。

故障分析

1. 检查各类业务流是否进入指定队列

   首先在 RouterA 上执行命令 **reset qos queue statistics interface gigabitethernet 0/0/1** 清除接口 GE0/0/1 上基于队列的流量统计信息。

   然后分别向 RouterA 发送语音、视频和数据等业务流，并执行命令 **display qos queue statistics**，查看接口上基于队列的流量统计信息。发现，语音、视频、数据的业务流均能按照配置进入指定队列，显示信息如下：

```
<RouterA> display qos queue statistics interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------
Queue                 Passed(Packets/Bytes)          Dropped(Packets/Bytes)
-------------------------------------------------------------------------------
Protocol                  0/0                            0/0
0                         0/0                            0/0
1                         0/0                            0/0
2                   3470/3470000                         0/0
3                         0/0                            0/0
4                         0/0                            0/0
5                   25600/256000                         0/0
6                   54354/5435400                        0/0
7                         0/0                            0/0
```

2. 检查各队列流量整形 CIR 之和是否大于基于接口的流量整形 CIR。

   在进入 RouterA 上的 WAN 接口视图，执行命令 **display this**，查看该接口上配置的流量整形参数。

```
[RouterA-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 qos queue-profile qq1
 qos gts cir 2000 cbs 50000
#
return
[RouterA-qos-queue-profile-qq1] display this
#
qos queue-profile qq1
  queue 2 gts cir 2000 cbs 50000
  queue 5 gts cir 500 cbs 12500
```


版权所有 © 华为技术有限公司

```
  queue 6 gts cir 100 cbs 2500
  queue 2 weight 20
  queue 5 weight 50
  schedule wfq 0 to 5 pq 6 to 7
#
return
```

显示信息表明，WAN 侧接口 GE0/0/1 上同时配置了基于接口的流量整形和基于队列的流量整形，队列 2、5 采用 WFQ 调度模式，队列 6 采用 PQ 调度，各队列流量整形参数均正确。但是，基于接口的流量整形 CIR 小于队列 2、5、6 的流量整形 CIR 之和。

AR2200-S 上，当基于接口的队列整形 CIR 小于各队列的流量整形 CIR 之和时，队列要求的承诺速率得不到保证。

操作步骤

步骤 1 在 RouterA 上执行命令 **interface gigabitethernet 0/0/1**，进入 WAN 接口视图。

步骤 2 执行命令 **qos gts cir 3000**，修改基于接口的流量整形的 CIR 为 3000kbps，使之大于各队列的流量整形 CIR 之和。

完成上述操作后，用户使用语音、视频、数据业务时，均能按组网要求保证其带宽。

----结束

案例总结

如果出现队列流量整形的结果不正确，则需重点关注接口上是否同时配置了基于接口的流量整形和基于队列的流量整形。如果同时配置，且基于接口的队流量整形 CIR 小于接口上各队列的流量整形 CIR 之和，队列要求的 CIR 将得不到保证。

9.5 拥塞避免故障处理

介绍拥塞避免相关故障的定位思路和典型案例。

9.5.1 拥塞避免不生效的定位思路

介绍拥塞避免不生效的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

拥塞避免不生效的常见原因包括：

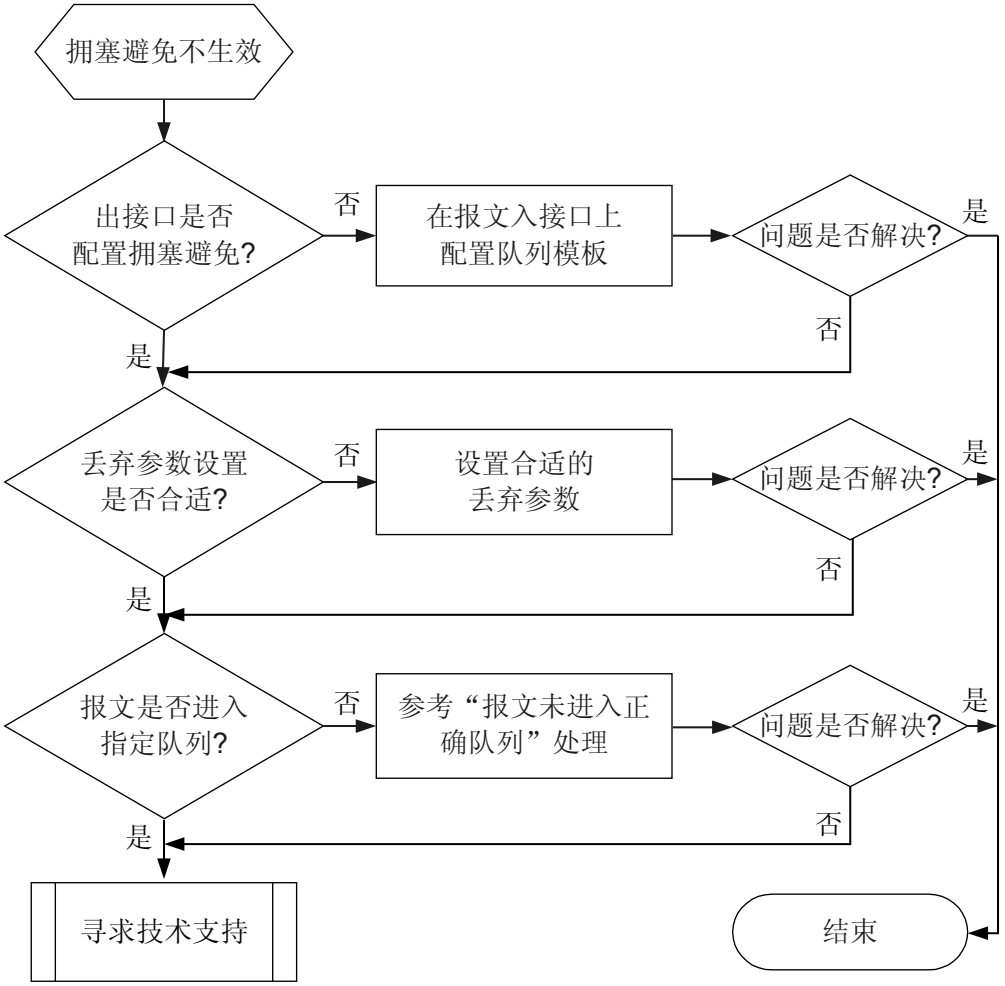
- 报文出接口没有配置拥塞避免。
- 丢弃参数设置不满足业务需求。
- 报文未进入指定队列。

故障诊断流程

如果拥塞避免不生效，请使用如图 9-11 所示的故障诊断流程处理。

版权所有 © 华为技术有限公司

图 9-11 拥塞避免不生效故障诊断流程图



故障处理步骤

说明

请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。

拥塞避免根据队列缓存长度和队列中报文实时长度判断是否丢弃，因此，如果上下门限和队列长度配置不合理，比如：队列长度过大，或上下门限过高，会影响拥塞避免效果，给人拥塞避免没有生效的错觉。

操作步骤

步骤 1 检查报文出接口上是否配置了拥塞避免

版权所有 © 华为技术有限公司

检查项	检查方法
是否配置了基于队列的拥塞避免	进入报文出接口视图，执行命令 **display this**，检查接口上是否配置有 **qos queue-profile** 命令。如果配置了，进入队列模板视图，执行命令 **display this**，检查指定队列是否配置了 **queue drop-profile** 命令。如果配置了，表明接口配置了基于队列的拥塞避免；否则，表明接口没有配置基于队列的拥塞避免。
是否配置基于流的拥塞避免	进入报文出接口视图，执行命令 **display this**，检查接口上是否配置有 **traffic-policy** 命令。如果配置了，进一步执行命令 **display traffic policy user-defined** 检查流策略中是否配置了 **drop-profile** 命令。如果配置了，表明接口配置了基于流的拥塞避免。否则，表明接口没有配置基于流的拥塞避免。

说明

只有 WAN 侧接口 CBWFQ 队列上才可配置基于流的拥塞避免。

- 如果即没有配置基于队列的拥塞避免，也没有配置基于流的拥塞避免，请根据需要在报文出接口配置基于队列的拥塞避免或配置基于流的拥塞避免。
- 如果配置了基于队列的拥塞避免或配置了基于流的拥塞避免，请执行步骤 2。

步骤 2 检查丢弃参数设置是否合适

执行命令 **display drop-profile**，查看丢弃模板中的丢弃参数，关注指定优先级的丢弃参数设置是否合适。

- 如果丢弃参数不合适（如丢弃上下限为 100，则采用尾丢弃，拥塞避免不会生效），请执行命令 **dscp discard-percentage** 或 **ip-precedence discard-percentage** 并按照业务需求修改丢弃上下限。
- 如果丢弃参数设置合适，请执行步骤 3

步骤 3 检查报文是否进入指定队列

执行命令 **display qos queue statistics interface**，查看报文出接口上的队列统计信息，看报文是否进入指定队列

- 如果报文没有进入指定队列，请参见 **9.2.1 报文未进入正确队列的定位思路**进行故障定位。
- 如果报文已进入指定队列，请执行步骤 5。

步骤 4 请收集如下信息，并联系华为技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警和日志

相关告警

无

相关日志

无

9.6 拥塞管理故障处理

介绍拥塞管理相关故障的定位思路和典型案例。

9.6.1 拥塞管理无效的定位思路

介绍拥塞管理无效的常见原因、故障诊断流程、故障处理步骤和相关告警与日志。

常见原因

本类故障的常见原因主要包括：

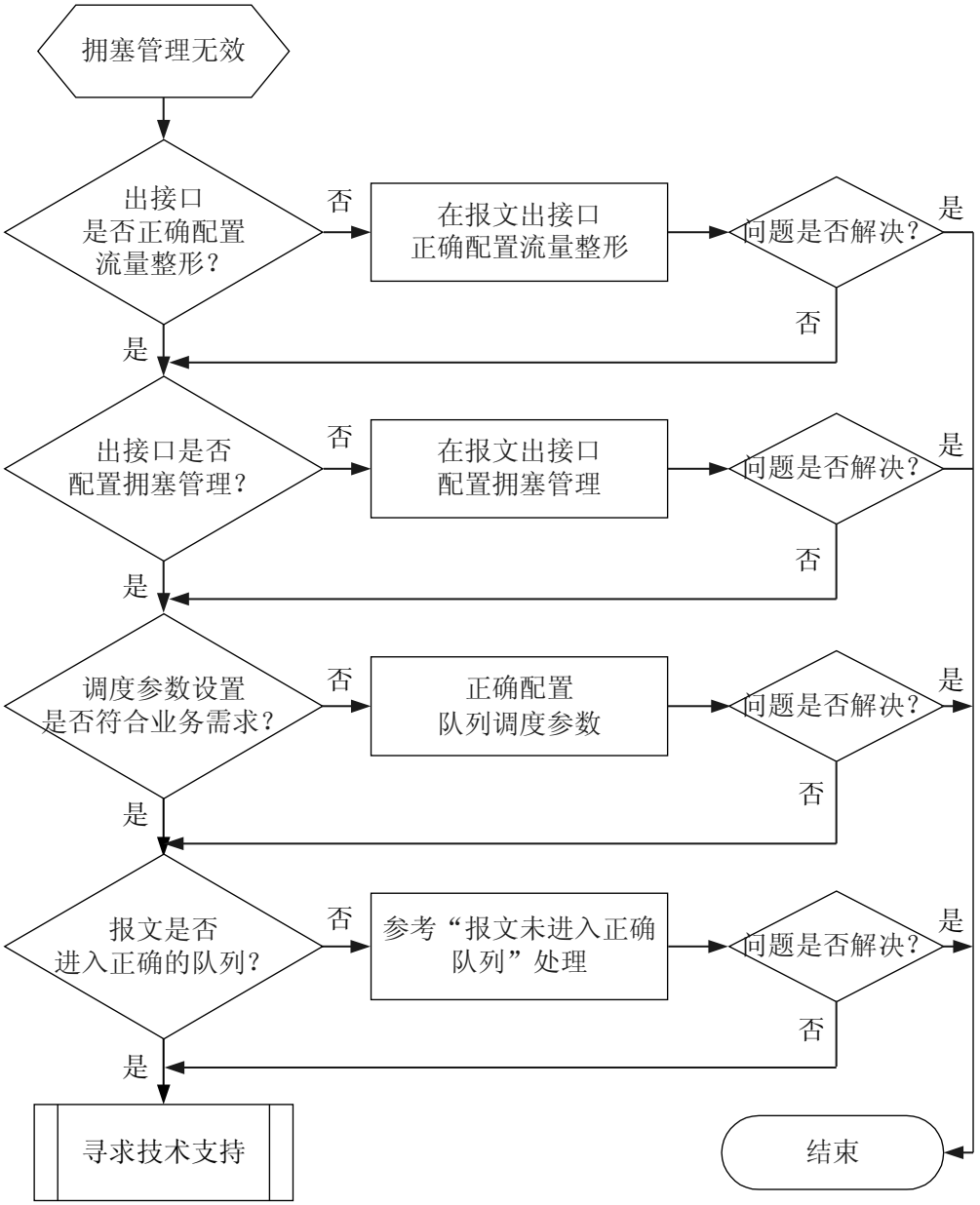
- 报文出接口没有配置基于接口的流量整形，致使接口无法产生拥塞。
- 报文出接口没有配置拥塞管理。
- 调度参数设置不符合业务需求。
- 报文未进入正确队列。

故障诊断流程

如果因某队列中的报文没有得到调度或调度不准而导致拥塞管理无效，请使用如**图 9-12** 所示的故障诊断流程处理。

版权所有 © 华为技术有限公司

图 9-12 拥塞管理无效故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查报文出接口是否正确配置流量整形

进入报文出接口视图，执行命令 **display this**，检查接口上是否配置有 **qos gts** 命令：

版权所有 © 华为技术有限公司

- 如果没有配置，或者配置的接口整形参数不符合业务需求，请执行命令 **qos gts** 正确配置。
- 如果已正确配置，请执行步骤 2。

步骤 2 检查报文出接口上是否配置了拥塞管理

检查项	检查方法
是否配置了基于队列的拥塞管理	进入报文出接口视图，执行命令 **display this**，检查接口上是否配置有 **qos queue-profile** 命令。如果配置了，进入队列模板视图，执行命令 **display this**，检查指定队列是否配置了 **schedule** 命令。如果配置了，表明接口配置了基于队列的拥塞管理；否则，表明接口没有配置基于队列的拥塞管理。
是否配置基于流的拥塞管理	进入报文出接口视图，执行命令 **display this**，检查接口上是否配置有 **traffic-policy** 命令。如果配置了，进一步执行命令 **display traffic policy user-defined** 检查流策略中是否配置了 **queue af**、**queue ef** 或 **queue wfq** 命令。如果配置了，表明接口配置了基于流的拥塞管理。否则，表明接口没有配置基于流的拥塞管理。

说明

只有 WAN 侧接口才可配置基于流的拥塞管理。

- 如果即没有配置基于队列的拥塞管理，也没有配置基于流的拥塞管理，请根据需要在报文出接口配置基于队列的拥塞管理或配置基于流的拥塞管理。
- 如果配置了基于队列的拥塞管理或配置了基于流的拥塞管理，请执行步骤 3。

步骤 3 检查调度参数设置是否符合业务需求

- 如果接口配置基于队列的拥塞管理，请进入队列模板视图，执行命令 **display this**，查看接口各队列的调度模式和权重，看其是否符合业务需求：

  说明

  缺省情况下，所有队列均采用 PQ 调度模式。当网络发生拥塞时，如果要均衡各类报文的延迟和延迟抖动，一般推荐：关键业务（如语音、视频）采用 PQ 调度，以确保业务优先处理；非关键业务（如 E-Mail）采用 DRR、WRR 或 WFQ 调度，以确保相同优先级业务得到公平处理，不同优先级业务按照各自权值处理。

  - 如果队列调度参数不符合业务需求，请执行命令 **schedule** 和 **queue weight**，重新规划各队列的调度模式和权重。
  - 如果队列调度参数符合业务需求，请执行步骤 4。
- 如果接口配置基于流的拥塞管理，请执行命令 **display traffic policy user-defined** 检查配置的调度方式、可确保的最小带宽等调度参数是否符合业务需求。
  - 如果调度参数不符合业务需求，请根据需要执行命令 **queue af**、**queue ef** 或 **queue wfq**，重新规划调度参数。
  - 如果调度参数符合业务需求，请执行步骤 4。

版权所有 © 华为技术有限公司

步骤 4 检查报文是否进入正确的队列

执行命令 **display qos queue statistics interface**，查看报文出接口上的队列统计信息，看报文是否进入指定队列：

说明

也可通过配置基于流策略的流量统计，然后执行命令 **display traffic policy statistics** 查看每条流入队列的统计信息，关注 **Passed** 和 **Dropped** 数目。有关基于流策略的流量统计的配置，请参见《企业路由器 配置指南-QoS》中的“配置流量统计”。

- 如果报文没有进入指定队列，请参见 9.2.1 报文未进入正确队列的定位思路进行故障定位。
- 如果报文进入指定队列，执行步骤 4。

步骤 5 请收集如下信息，并联系华为技术支持工程师

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警和日志

相关告警

无

相关日志

无

9.6.2 故障处理案例

介绍拥塞管理相关的典型故障案例。

网络拥塞导致业务断断续续

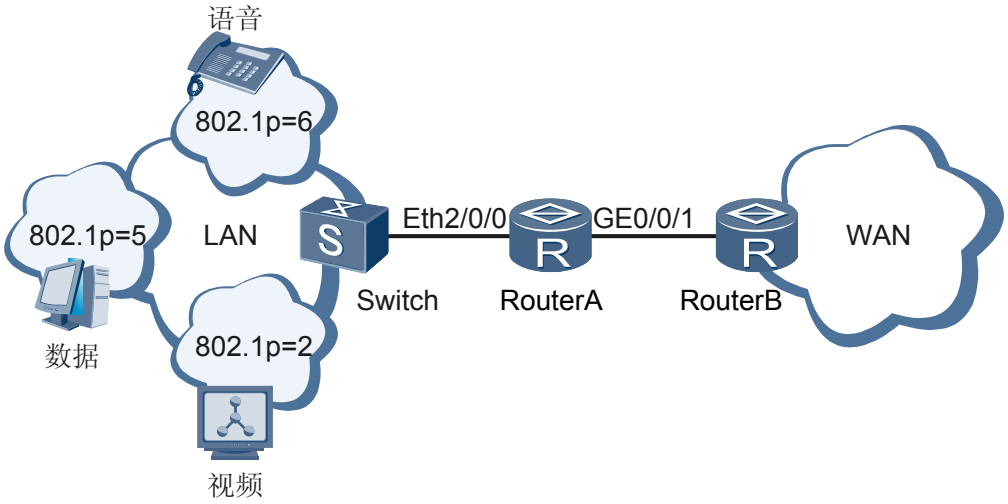
网络环境

在如图 9-13 所示组网中。由于来自 LAN 侧的流量速率大于 WAN 接口的速率，Router 的下行接口 GE0/0/1 处可能会发生拥塞。为避免拥塞，保证各类业务的带宽要求，在 Router 上配置使语音、视频、数据的业务流分别进入队列 6、2、5，并配置队列拥塞管理功能，使：

- WAN 侧出接口带宽为 10000kbps。
- 语音最大带宽为 3000kbps。
- 视频和数据报文分享剩余带宽，比例为 5:2。
- 语音业务流对应的 6 号采用 PQ 调度；视频、数据业务流对应的 2、5 号队列采用 WFQ 调度，权重分别为 50、20。

版权所有 © 华为技术有限公司

图 9-13 网络拥塞导致业务断断续续故障案例组网图



配置完成后，发现视频、数据业务流出现断断续续的现象，得不到优质服务，拥塞管理功能无效。

故障分析

1. 检查 Router 的下行接口上是否正确配置了流量整形和队列调度参数。

   进入 GE0/0/1 接口视图，执行命令 **display this**，查看接口配置。

   ```
   [Router-GigabitEthernet0/0/1] display this
   #
   interface GigabitEthernet0/0/1
    ip address 192.168.0.1 255.255.255.0
    qos queue-profile qq1
    qos gts cir 10000 cbs 250000
   #
   return
   ```

   显示信息表明，GE0/0/1 接口上配置了基于接口的流量整形，并绑定队列模板 **qq1**，基于接口的流量整形配置正确。

2. 检查队列调度模板中是否正确配置了队列流量整形参数和队列调度参数。

   进入队列模板视图，执行命令 **display this**，查看配置的队列流量整形参数和队列调度参数。

   ```
   [Router-qos-queue-profile-qq1] display this
   [V200R001C00B130]
   #
   qos queue-profile qq1
     queue 7 gts cir 3000 cbs 75000
     queue 2 weight 50
     queue 5 weight 20
     schedule wfq 0 to 5 pq 6 to 7
   #
   ```

   显示信息表明，2、5 队列采用 WFQ 调度，6、7 队列采用 PQ 调度，2、5 队列调度权重分别为 50、20，7 队列配置流量整形 CIR 为 3000kbps。由于语音业务流进入的是 6 队列，但 6 队列没有配置流量整形，导致语音业务流可能会抢占端口所有带宽，从而会使视频、数据业务中断。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 在 Router 上执行命令 **system－view**，进入系统视图。

步骤 2 执行命令 **qos queue-profile qq1**，进入队列模板 **qq1** 的视图。

步骤 3 执行命令 **undo queue 7 gts**，取消对 7 队列的流量整形。

步骤 4 执行命令 **queue 6 gts cir 3000**，配置对 6 队列进行流量整形，整形带宽为 3Mbps。

完成上述操作后，用户使用语音、视频、数据业务时，均能按组网要求保证其带宽。

----结束

案例总结

在配置拥塞管理时，如果队列采用混合调度模式，需要注意对采用 PQ 调度的队列进行带宽限制。因为，在混合调度模式下，AR2200-S 先调度 PQ 队列，PQ 队列调度完成后，再对 DRR、WFQ 或 WRR 队列进行加权轮循调度。这样，如果 PQ 队列没有带宽限制，PQ 队列的业务流可能会抢占整个接口的带宽，从而会导致其他队列中的业务得不到服务或中断。

版权所有 © 华为技术有限公司

10 安全类

关于本章

10.1 AAA 故障处理
10.2 ARP 安全故障处理
10.3 NAC 故障处理
10.4 DHCP Snooping 故障处理
10.5 防火墙故障处理
10.6 ACL 故障处理
10.7 NAT 故障处理
10.8 PKI 故障处理

版权所有 © 华为技术有限公司

10.1 AAA 故障处理

10.1.1 RADIUS 用户认证失败的定位思路

常见原因

本类故障的常见原因主要包括：

- 用户名或密码不正确，包括用户名不存在，或用户名传给 RADIUS 服务器时对域名的处理方式与服务器配置的不一致
- AR2200-S 的 RADIUS 配置错误，包括认证模式、服务器模板
- RADIUS 服务器端的端口、共享密钥和 AR2200-S 的配置不一致
- 当前上线用户数已经达到定义的最大值

故障诊断流程

在 AR2200-S 上配置 RADIUS 后，发现用户不能通过 RADIUS 认证。

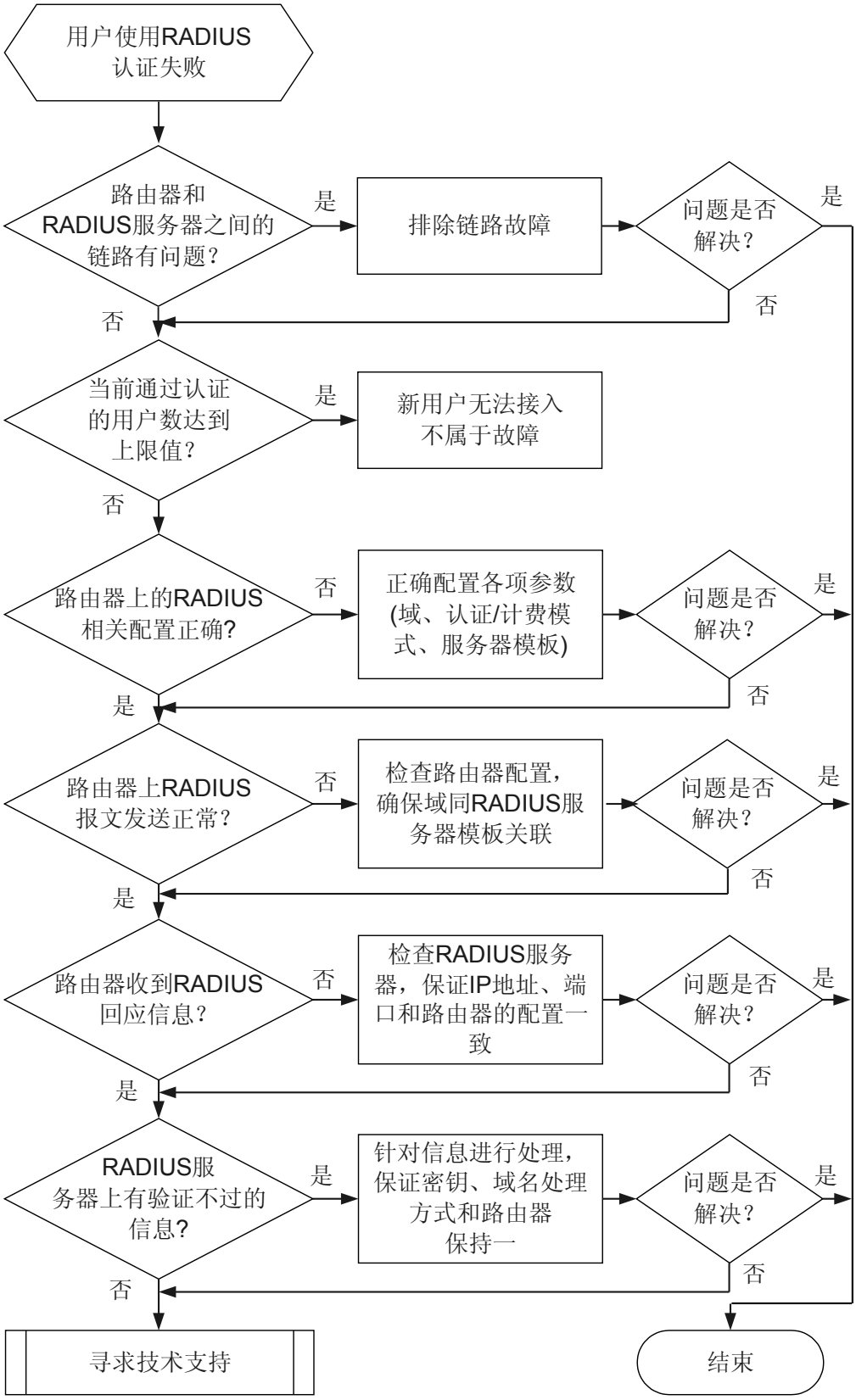
故障的定位思路如下：

- 检查 AR2200-S 和 RADIUS 服务器的链路连接是否正常
- 检查当前通过认证的用户数是否达到上限值
- 检查 AR2200-S 上的 RADIUS 配置是否正确，包括域名、域状态、服务器模板、认证模式、计费模式
- 检查 RADIUS 服务器是否正常，包括服务器上配置的用户名、密码、用户接入类型是否正确，配置的接入设备的 IP 地址、端口、共享密钥、域名携带及解析方式是否和 AR2200-S 的配置一致

详细处理流程如图 10-1 所示。

版权所有 © 华为技术有限公司

图 10-1 RADIUS 用户认证失败的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 通过 **ping** 检查路由器与 RADIUS 服务器之间的路由是否有故障。

- 如果 ping 不通，请先根据 **7.1.1 Ping 不通问题的定位思路**排除路由的故障。
- 如果能 ping 通，请执行步骤 2。

步骤 2 检查在线用户数是否达到了定义的最大值。

路由器和 RADIUS 服务器对接入的用户数都有规格限制。在 AR2200-S 上使用 **display access-user** 命令，查看通过认证在线的用户数。

- 如果已经达到了定义的最大值，那么新用户无法接入是正常的。
- 如果在线用户没有达到最大上限，再去 RADIUS 服务器上查看是否有限制。如果排除了服务器上的限制问题后，用户还是无法通过认证，请执行步骤 3。

步骤 3 检查 AR2200-S 的 RADIUS 相关配置。

- 查看用户认证的域状态是否为 Active。
- 查看域下绑定的认证方案中认证模式是否为 RADIUS 认证。
- 查看域下绑定的 RADIUS 服务器模板是否正确；该模板的认证服务器、计费服务器的地址、端口是否正确；路由器发送报文携带的源地址是否和服务器上配置允许接入的地址一致。
- 查看 RADIUS 服务器模板中对用户名格式的处理和共享密钥是否和 RADIUS 服务器上的配置一致。

后两项检查要结合 RADIUS 服务器的检查一起进行，请参考步骤 4。根据实际组网环境，保证上面各项的配置符合要求。

查看项目	使用命令
查看域	**display domain**
查看域下绑定的模板	**display domain name** *domain-name*
查看认证方案	**display authentication-scheme**
查看计费方案	**display accounting-scheme**
查看模板中配置的信息	**display radius-server configuration**

步骤 4 检查 RADIUS 报文收发是否正常。

在 AR2200-S 的用户视图下执行命令 **debugging radius packet** 打开 RADIUS 调试信息开关，发起 RADIUS 认证，或者用 **test-aaa** 命令发送认证请求，观察是否有 RADIUS 报文的发送和接收。

```
<Huawei> debugging radius packet
<Huawei> terminal debugging
<Huawei> terminal monitor
```


版权所有 © 华为技术有限公司

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

- 如果打开调试开关后没有任何信息，说明设备的网络接入配置有问题。重点检查域是否同 RADIUS 服务器模板关联起来。

  如下配置文件所示，域 **huawei** 下绑定了 RADIUS 服务器模板 **radius**。

```
#
radius-server template radius
 radius-server authentication 1.1.1.1 1645
#
aaa
 authentication-scheme default
 authentication-scheme aaa
  authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme aaa
  radius-server  radius
```

- 如果看到有调试信息，根据调试信息的内容进行处理。

调试信息	处理方法

Nov 10 2010 15:23:34.260.6 Huawei RDS/7/ debug2:
  Radius Sent a Packet
  Server Template: 0
  Server IP : 192.168.1.128
  Protocol: Standard
  .....
	这是 RADIUS 模块发送的认证报文的信息，该信息表明 AR2200-S 上的 RADIUS 认证报文能正常向外发送。

Nov 10 2010 15:23:34.260.6 Huawei %%01RDS/4/ RDAUTHDOWN(l): RADIUS authentication server (IP: 192.168.1.128) is down!	该信息表明 RADIUS 认证服务器没有认证回应消息，可能是链路不通或者 RADIUS 认证服务器没有启动。 需要检查 RADIUS 服务器的配置，保证服务器上的路由器 IP 地址、端口号和对端一致，并且服务器上相关端口的服务已经启动。

版权所有 © 华为技术有限公司

调试信息	处理方法
Nov 10 2010 15:23:34.260.6 Huawei RDS/7/debug2: [RDS (Evt):] Send a msg (Auth reject) Nov 10 2010 15:23:34.260.7 Huawei RDS/7/debug2: [RDS (Msg):]Msg type :Auth reject [RDS (Msg):]UserID :16005 [RDS (Msg):]Template no:88.99 [RDS (Msg):]Authmethod :(pap) [RDS (Msg):]ulSrcMsg :Auth req [RDS (Msg):]szBitmap :00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	这是 RADIUS 认证失败回应报文。可能原因有： ● RADIUS 服务器没有配置路由器的地址和共享密钥。 ● RADIUS 服务器和路由器两端配置的共享密钥不一致。 ● RADIUS 服务器没有配置该用户。需要注意路由器上配置的服务器模板是否会对登录用户名进行域名剥离处理。 ● RADIUS 服务器上该用户的密码和登录用户的密码不一致。 根据实际组网环境，保证 RADIUS 服务器端的配置都符合要求。通过以上处理，大部分的认证不通过问题都可以得到解决。如果问题仍然存在，请执行步骤 5。

步骤 5 根据被拒绝的用户属于哪一种用户类型，采取相应的下一步措施。

- 如果是 Telnet 用户或 FTP 用户，请参考 **2.2.1 Telnet 登录失败的定位思路**、FTP 登录失败的定位思路。
- 如果是接入用户，请参考 **10.3 NAC 故障处理**。

步骤 6 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.1.2 HWTACACS 用户认证失败的定位思路

常见原因

本类故障的常见原因主要包括：

版权所有 © 华为技术有限公司

- 用户名或密码不正确，包括用户名不存在，或用户名传给 HWTACACS 服务器时对域名的处理方式与服务器配置的不一致
- AR2200-S 的 HWTACACS 配置错误，包括认证模式、服务器模板
- HWTACACS 服务器端的端口、共享密钥和 AR2200-S 的配置不一致
- 当前上线用户数已经达到定义的最大值

故障诊断流程

在 AR2200-S 上配置 HWTACACS 后，发现用户不能通过 HWTACACS 认证。

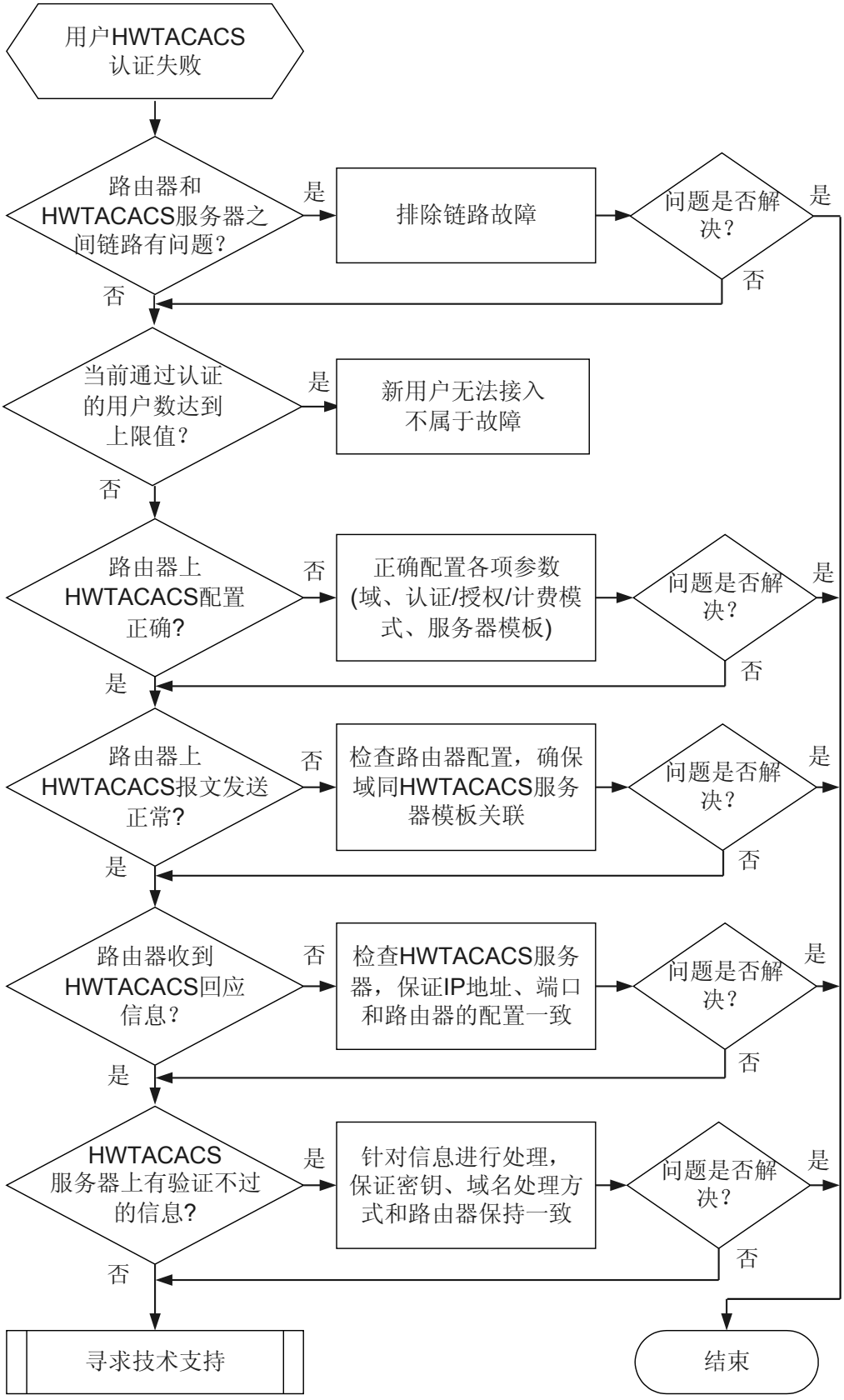
故障的定位思路如下：

- 检查 AR2200-S 和 HWTACACS 服务器的链路连接是否正常
- 检查当前通过认证的用户数是否达到上限值
- 检查 AR2200-S 上的 HWTACACS 配置是否正确，包括认证模式、授权模式、计费模式、域名、域状态、服务器模板
- 检查 HWTACACS 服务器是否正常，包括服务器上配置的用户名、密码、用户接入类型是否正确，配置的路由器 IP 地址、端口、共享密钥、域名携带及解析方式是否和 AR2200-S 的配置一致

详细处理流程如**图 10-2** 所示。

版权所有 © 华为技术有限公司

图 10-2 HWTACACS 用户认证失败的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 通过 **ping** 检查路由器与 HWTACACS 服务器之间的路由是否有故障。

- 如果 ping 不通，请先根据 **7.1.1 Ping 不通问题的定位思路**排除路由的故障。
- 如果能 ping 通，请执行步骤 2。

步骤 2 检查在线用户数是否达到了定义的最大值。

路由器和 HWTACACS 服务器对接入的用户数都有规格限制。在 AR2200-S 上使用 **display access-user** 命令，查看通过认证在线的用户数。

- 如果已经达到了定义的最大值，那么新用户无法接入是正常的。
- 如果在线用户没有达到最大上限，再去 HWTACACS 服务器上查看是否有限制。如果排除了服务器上的限制问题后，用户还是无法通过认证，请执行步骤 3。

步骤 3 检查 AR2200-S 设备的 HWTACACS 配置。

- 查看用户认证的域状态是否为 Active。
- 查看域下绑定的认证方案中认证模式是否为 HWTACACS 认证。
- 查看域下绑定的 HWTACACS 服务器模板是否正确；该模板的认证服务器、授权服务器、计费服务器的地址、端口是否正确；路由器发送报文携带的源地址是否和服务器上配置允许接入的地址一致。
- 查看 HWTACACS 服务器模板中对用户名格式的处理和共享密钥是否和 HWTACACS 服务器上的配置一致。

后两项检查要结合 HWTACACS 服务器的检查一起进行，请参考步骤 4。根据实际组网环境，保证上面各项的配置符合要求。

查看项目	使用命令
查看域	**display domain**
查看域下绑定的模板	**display domain name** *domain-name*
查看认证方案	**display authentication-scheme**
查看授权方案	**display authorization-scheme**
查看计费方案	**display accounting-scheme**
查看模板中配置的信息	**display hwtacacs-server template**

步骤 4 检查 HWTACACS 报文收发是否正常。

在 AR2200-S 的用户视图下执行命令 **debugging hwtacacs all** 打开 HWTACACS 调试信息开关，发起 HWTACACS 认证，观察是否有 HWTACACS 报文的发送和接收。

版权所有 © 华为技术有限公司

```
<Huawei> debugging hwtacacs all
<Huawei> terminal debugging
<Huawei> terminal monitor
```

注意

打开调试开关将影响系统的性能。调试完毕后，应及时执行 **undo debugging all** 命令关闭调试开关。

- 如果打开调试开关后没有任何信息，说明设备的网络接入配置有问题。重点检查域是否同 HWTACACS 服务器模板关联起来。

  如下配置文件所示，域 **huawei** 下绑定了 HWTACACS 服务器模板 **hwtacacs**。

```
#
hwtacacs-server template hwtacacs
 hwtacacs-server authentication 2.2.2.2
#
aaa
 authentication-scheme default
 authentication-scheme aaa
  authentication-mode hwtacacs
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme aaa
  hwtacacs-server hwtacacs
#
```

- 如果看到有调试信息，根据调试信息的内容进行处理。

调试信息	处理方法
Nov 10 2010 15:43:35.500.6 Huawei TAC/7/ Event:HandleReqMsg: Session status is not connect now. Nov 10 2010 15:43:35.500.7 Huawei TAC/7/ Event:statistics: transmit flag: 1-SENDPACKET, server flag: 0-authentication, packet flag: 0xff Nov 10 2010 15:43:35.550.1 Huawei TAC/7/ Event:HandleResp: Session status is connect now. Nov 10 2010 15:43:35.550.2 Huawei TAC/7/ Event: Tac packet sending success! version:c0 type:1-authentication sequence:1 flag:1-UNENCRYPTED_FLAG session id:908 length:24 serverIP:10.138.88.209 vrf:0	这是 HWTACACS 模块发送的认证报文的信息，该信息表明 AR2200-S 发送 HWTACACS 认证报文成功。
Nov 10 2010 15:49:18.430.6 Huawei TAC/7/ Event:HandleReqMsg: Session status is not connect now. Nov 10 2010 15:49:18.430.7 Huawei TAC/7/ Event:statistics: transmit flag: 1-SENDPACKET, server flag: 0-authentication, packet flag: 0xff Nov 10 2010 15:49:18.480.2 Huawei TAC/7/ Event:HandleResp: Session status is connect now. Nov 10 2010 15:49:18.480.3 Huawei TAC/7/ Event: Tac send packet error!	该信息表明 HWTACACS 认证服务器没有回应认证消息，可能是 HWTACACS 服务器没有启动、过期无效或者链路不通。 需要检查 HWTACACS 服务器的配置，保证服务器上的路由器 IP 地址、端口和对端一致，并且服务器上相关端口的服务已经启动。

版权所有 © 华为技术有限公司

调试信息	处理方法
Nov 10 2010 16:02:35.760.1 Huawei TAC/7/ Event: version:c0 type:AUTHEN_REPLY seq_no:6 flag:UNENCRYPTED_FLAG session_id:0x4ff8 length:6 pstPacketAll->ulDataLen:6 pstAuthenReply:ucStatus=2 ucflags=0 usServerMsgLen=0 usDataLen=0 status:AUTHEN_STATUS_FAIL flag:REPLY_FLAG_ECHO server_msg len:0 data len:0 server_msg: data:	这是 HWTACACS 服务器回应认证拒绝消息。可能原因有： ● HWTACACS 服务器没有配置路由器的地址和共享密钥。 ● HWTACACS 服务器和路由器配置的共享密钥不一致。 ● HWTACACS 服务器没有配置该用户。需要注意路由器上配置的服务器模板是否会对登录用户名进行域名剥离处理。 ● HWTACACS 服务器上该用户的密码和登录用户的密码不一致。 根据实际组网环境，保证 HWTACACS 服务器端的配置都符合要求。通过以上处理，大部分的认证不通过问题都可以得到解决。如果问题仍然存在，请执行步骤 5。

步骤 5 根据被拒绝的用户属于哪一种用户类型，采取相应的下一步措施。

- 如果是 Telnet 用户或 FTP 用户，请参考 **2.2.1 Telnet 登录失败的定位思路**、FTP 登录失败的定位思路。
- 如果是接入用户，请参考 **10.3 NAC 故障处理**。

步骤 6 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.1.3 故障案例

用户登录设备十几秒内被强制下线

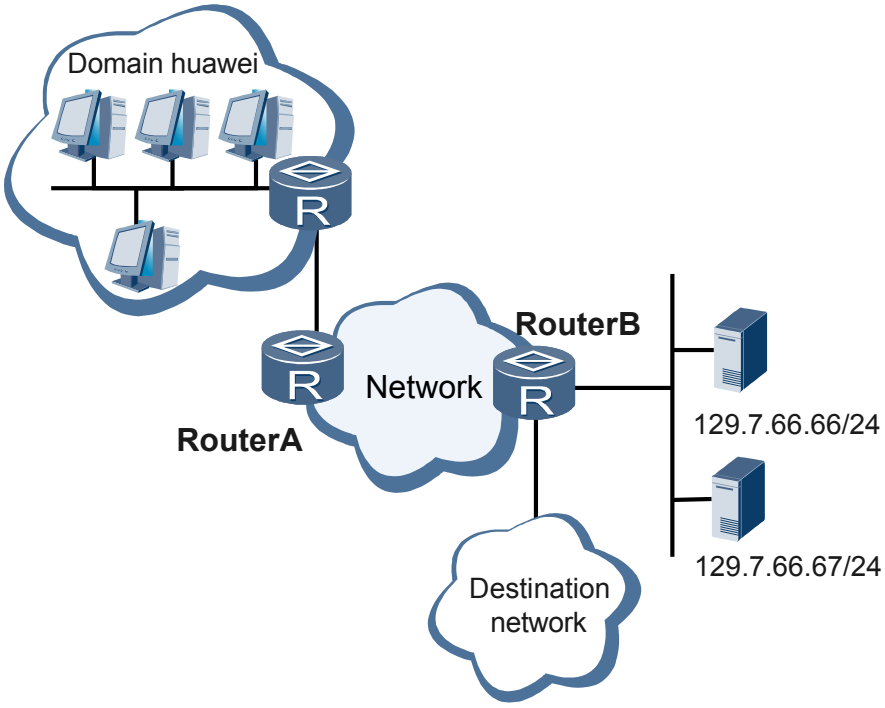
版权所有 © 华为技术有限公司

网络环境

在图 10-3 所示的网络中，用户通过网络接入服务器 RouterB 访问网络，在 RouterB 上对用户登录进行认证、授权和计费。

RouterB 原来使用 RADIUS 协议对用户进行认证和计费，由于 RADIUS 服务器故障，配置管理员采用本地认证。

图 10-3 用户登录设备十几秒内被强制下线组网图



配置完成后，发现用户登录设备十几秒内被强制下线。

故障分析

1. 在 RouterB 上执行 **display trapbuffer** 和 **display logbuffer** 命令，查看是否有强制用户下线的告警和日志信息。发现有如下告警信息：

   ```
   AAA cut user!
   ```

2. 在 RouterB 上执行 **display current-configuration** 命令，查看 AAA 的配置信息。发现 AAA 采用了本地认证和远端计费，配置如下：

   ```
   radius-server template provera
    radius-server shared-key simple 123456
    radius-server authentication 129.7.66.66 1812
    radius-server accounting 129.7.66.66 1813
    undo radius-server user-name domain-included
   #
   aaa
    local-user telenor password OUM!K%F<+$[Q=^Q`MAF4<1!!
    authentication-scheme default
    #
    authentication-scheme provera
     authentication-mode  radius  local
    #
    authorization-scheme default
   ```


版权所有 © 华为技术有限公司

```
#
accounting-scheme default
accounting-scheme provera
 accounting-mode radius
 accounting realtime 10
#
domain default
#
domain huawei
 authentication-scheme  provera
 accounting-scheme provera
 radius-server provera
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
 set authentication password cipher %$%$#WXTFLJ\$/[lnd8G!:#Q,B9O{Cv8T8VJr7=S+/@a$Q!%7H~:%$%$
 history-command max-size 256
 screen-length 15
```

由于 RADIUS 服务器不可用，会导致实时计费失败。实时计费失败时，用户可以通过执行命令 **accounting interim-fail** 配置实时计费失败的策略，继续让用户在线或者强制用户下线。由于没有配置该命令，设备采用缺省情况，即实时计费失败时强制用户下线。

因此，是由于采用 RADIUS 计费失败导致用户下线。用户被强制下线的时间由超时重传时间和超时重传次数决定，这两个参数由命令 **radius-server**{ **retransmit** *retry-times* | **timeout** *time-value* }*配置。重传时间缺省是 5 秒，重传次数缺省是 3 次，因此用户登录 15 秒后就会被强制下线。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain huawei**，进入 huawei 域视图。

步骤 4 执行命令 **undo accounting-scheme provera**，配置域采用缺省计费模式，即不计费。

要排除以上故障可以选择以下三种方法之一：

- 执行命令 **accounting-mode none**，将计费方式改为不计费。
  针对 Telnet、FTP 等管理型用户时，不涉及收费，可以改用不计费模式。
- 执行命令 **accounting interim-fail online**，配置实时计费失败时用户继续在线。
- 执行命令 **undo accounting-scheme provera**，配置域采用缺省计费模式，即不计费。

经分析后，这里主要是针对 Telnet 等管理型用户进行认证，不需要计费，因此采用不计费策略。即执行命令 **undo accounting-scheme provera**。

完成上述操作后，用户重新登录，不再掉线，故障排除。

----结束

案例总结

在接入网络中，通过 AAA 验证用户登录设备时，如果远端服务器不可用需要暂时使用本地认证时，计费方案必须是不计费，否则将导致用户下线。

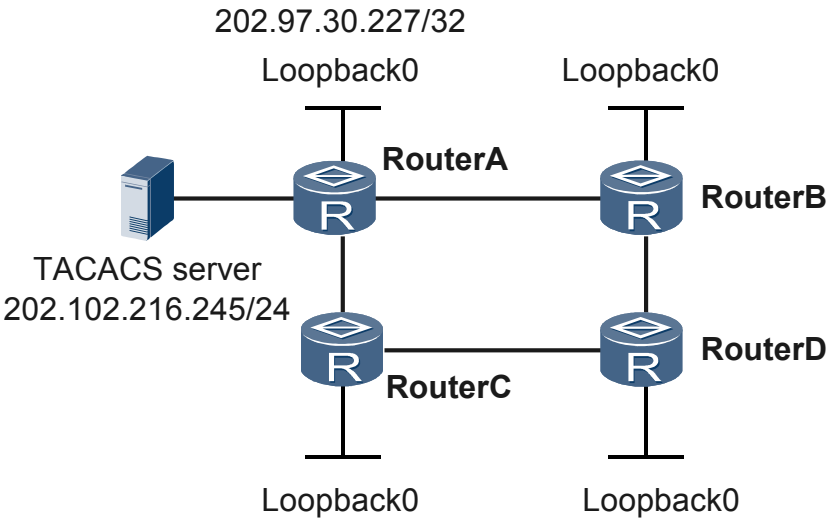
合法的用户名和密码不能通过 HWTACACS 认证

版权所有 © 华为技术有限公司

网络环境

在图 10-4 所示的网络，在网络的核心节点部署了路由协议、AAA、QoS、SNMP 等业务，其中四台路由器属于同一个 AS 域，路由协议采用 IBGP、ISIS。现按照客户规划新的私有 AS 号重新配置路由器，将 IBGP 改为 EBGP，将 IGP 的 ISIS 改为 OSPF 协议。其中 ISIS 协议中只包括互连接口和 Loopback 接口的 IP 地址。

图 10-4 合法的用户名和密码不能通过 HWTACACS 认证组网图



配置完成后，原来合法的 HWTACACS 用户名和密码不能通过 HWTACACS 认证。

故障分析

1. 检查 HWTACACS Server 记录的用户名和密码与用户使用的是否一致，发现用户名和密码正确。
2. 在 RouterA 上执行 **ping** 命令，检查路由器和 HWTACACS Server 是否互通，发现能够 ping 通。
3. 在 RouterA 上执行 **display current-configuration** 命令，检查 HWTACACS 的配置是否正确。发现在 HWTACACS 服务器模板中配置了如下命令：

   ```
   hwtacacs-server source-ip 202.97.30.227
   ```

   其中，202.97.30.227 是 RouterA 的 Loopback 接口地址。

   由于删除的 ISIS 协议中包括 Loopback 接口发布的路由，并且 HWTACACS 使用 RouterA 的 Loopback 接口地址作为源 IP，因此考虑可能是路由器无法收到 HWTACACS Server 返回的以 202.97.30.227 为目的地址的认证响应报文，导致 HWTACACS 认证失败。
4. 在 RouterA 上执行 **ping -a 202.97.30.227 202.102.216.245** 命令（202.102.216.245 是 HWTACACS Server 的 IP 地址），检查该 Loopback 地址和 HWTACACS Server 是否互通，发现不能 ping 通。
5. 在 RouterA 上执行 **display ip routing-table** 命令，检查路由协议是否发布了该 Loopback 接口的 IP 地址，发现 Loopback0 接口的 IP 地址没有发布。

版权所有 © 华为技术有限公司

因此，确认是网络调整中删除 ISIS 协议，发布 Loopback 接口的配置也被删除，且 OSPF 协议中没有发布该 Loopback 接口的地址，路由器无法接收 HWTACACS Server 返回的认证响应报文，导致认证失败。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ospf** *process-id*，进入 OSPF 视图。

步骤 3 执行命令 **area** *area-id*，进入 OSPF 区域视图。

步骤 4 执行命令 **network** *address wildcard-mask*，发布该 Loopback 接口的 IP 地址。

完成上述操作后，使用该用户名和密码，可以正常登录，故障排除。

----结束

案例总结

网络设备协议数据调整前，请记录之前的相关配置。协议数据调整后，检查调整后数据是否满足协议调整前的需求，并且检查是否对其他配置产生影响。

RADIUS 服务器未配置用户导致 Telnet 用户无法登录

网络环境

AR2200-S 设备启用 802.1x，用户接入需要进行 RADIUS 认证。配置后，802.1x 用户认证正常，但 Telnet 用户无法登录设备。

故障分析

1. 802.1x 用户认证正常，说明 AR2200-S 和 RADIUS 服务器的连接没有问题。
2. AR2200-S 上执行命令 **display current-configuration**，查看当前系统配置。

```
.....
 dot1x enable
#
radius-server template remote
 radius-server shared-key simple 123456
 radius-server authentication 192.168.1.27 1812
 radius-server accounting 192.168.1.27 1813
#
.....
interface Ethernet2/0/0
 port hybrid pvid vlan 10
 dot1x enable
 dot1x max-user 1
 dot1x port-method port
 dot1x reauthenticate
.....
aaa
 authentication-scheme default
 authentication-scheme cams
  authentication-mode  radius
 #
 authorization-scheme default
 authorization-scheme cams
  authorization-mode  none
 #
```


版权所有 © 华为技术有限公司

```
 accounting-scheme default
 accounting-scheme account
 accounting-scheme cams

 #
 domain default
  authentication-scheme  cams
  authorization-scheme cams
  accounting-scheme cams
  radius-server remote
 #
 domain default_admin
  authentication-scheme  cams
  authorization-scheme cams
  accounting-scheme cams
  radius-server remote
#
......
#
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
 authentication-mode aaa
 user privilege level 15
 idle-timeout 0 0
#
```

从以上信息中可以看出，用户登录时使用“default”域进行认证授权，认证模式使用 RADIUS 认证，授权方式为不需授权（none）。802.1x 用户认证正常，从 802.1x 的配置中可以看出，802.1x 用户基于端口进行认证。Telnet 用户使用“default_admin”域进行认证授权，其下配置与“default”域相同，使用 RADIUS 认证。用户登录失败，可能是 RADIUS 服务器上没有针对 Telnet 用户的用户名和密码。

3. 在 RADIUS 服务器上检查配置，发现没有创建该 Telnet 用户的用户名。

可以通过在 RADIUS 服务器上添加 Telnet 用户名和密码或者让 Telnet 用户使用本地认证来解决故障。

操作步骤

- 在 RADIUS 服务器上添加 Telnet 用户名和密码。配置方法请参见 RADIUS 服务器的配置指导书。
- 在 AR2200-S 上配置 Telnet 用户使用本地认证。

  创建新的域供 Telnet 用户使用。

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain telnet
[Huawei-aaa-domain-telnet]
```

  域下使用缺省的认证、授权、计费方案（缺省的认证方案为本地认证，授权方案为本地授权，计费方案为不计费）。

```
<Huawei> display domain name telnet

  Domain-name                    : telnet
  Domain-state                   : Active
  Authentication-scheme-name     : default
  Accounting-scheme-name         : default
  Authorization-scheme-name      : -
  Service-scheme-name            : -
  RADIUS-server-template         : -
  HWTACACS-server-template       : -
```


版权所有 © 华为技术有限公司

```
<Huawei> display authentication-scheme default

  Authentication-scheme-name    : default
  Authentication-method         : Local
  Authentication-super method   : Super authentication-super
<Huawei> display authorization-scheme default
------------------------------------------------------------------------------
 Authorization-scheme-name   : default
 Authorization-method        : Local
......
<Huawei> display accounting-scheme default

  Accounting-scheme-name               : default
  Accounting-method                    : None
```

创建用户时带上域名，Telnet 用户登录时要带域名输入用户名。

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user telnetuser@telnet password 123456
[Huawei-aaa] local-user telnetuser@telnet service-type telnet
```

----结束

案例总结

对于接入用户（例如 8021.x 用户）和 Telnet 用户、SSH 用户建议采用不同的认证方法。当 Telnet 用户不能登录设备时，常见原因多是由于在 VTY 用户界面视图、AAA 视图及远端的认证服务器中配置了不匹配的认证方式。

10.2 ARP 安全故障处理

10.2.1 合法用户的 ARP 表项被修改的定位思路

常见原因

本类故障的常见原因主要包括：

- 攻击者伪造合法用户的 ARP 报文修改合法用户的 ARP 表项

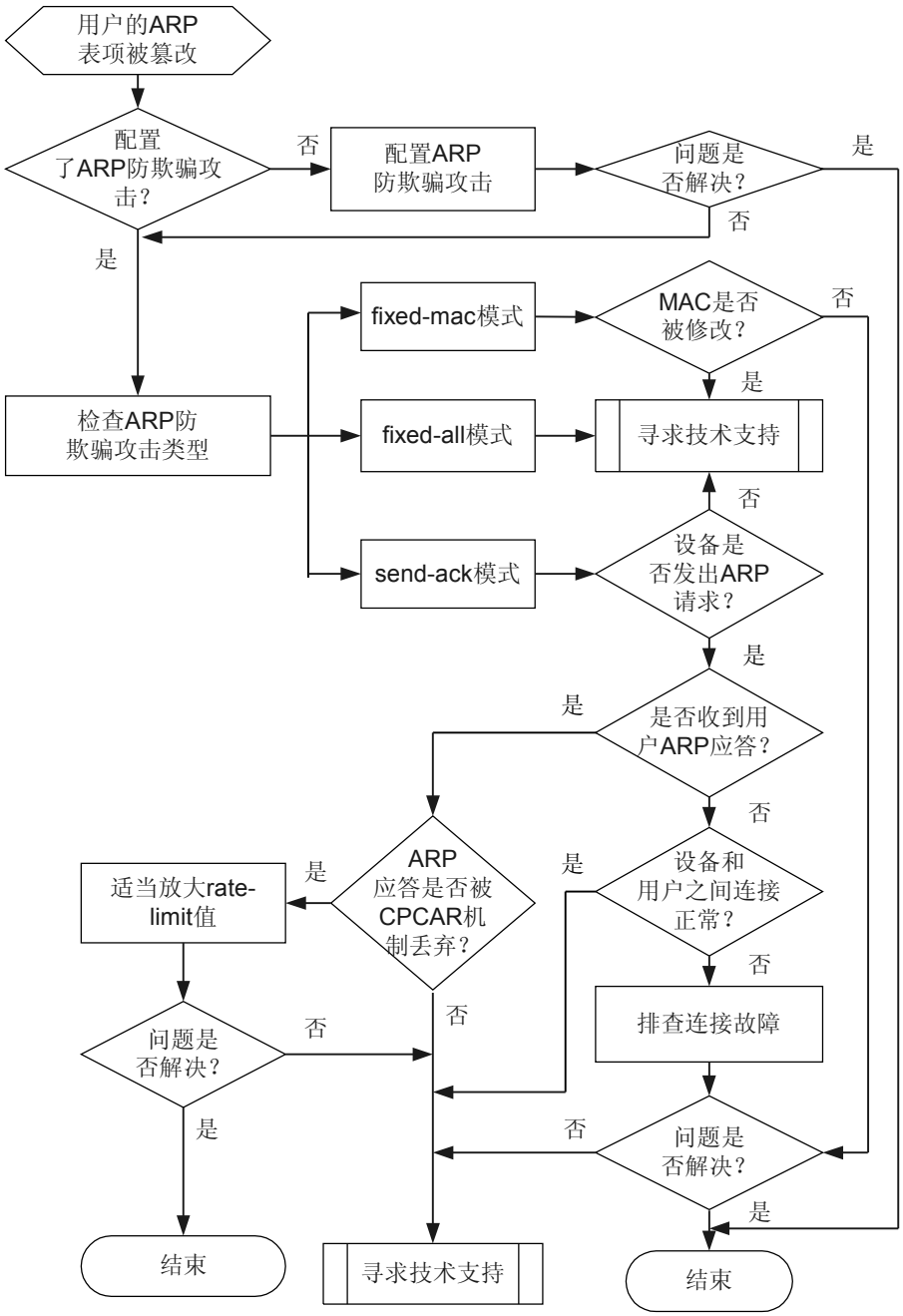
故障诊断流程

合法用户的网络服务突然中断，初步排查不是链路连接或路由问题。可能是攻击者通过伪造其他用户发出的 ARP 报文，篡改网关设备上的用户 ARP 表项，造成其他合法用户的网络服务中断。以下描述基于 ARP 表项被修改的处理流程。

详细处理流程如图 10-5 所示。

版权所有 © 华为技术有限公司

图 10-5 合法用户 ARP 表项被修改故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 在 AR2200-S 上执行命令 **display arp anti-attack configuration entry-check** 查看 ARP 防地址欺骗功能是否使能。

版权所有 © 华为技术有限公司

- 如果显示如下信息，则表示没有使能防 ARP 防地址欺骗功能。
  ```
  ARP anti-attack entry-check mode: disabled
  ```
  执行 **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable** 命令，使能该功能。

  说明

  在使能该功能前需要执行 **reset arp interface** *interface-type interface-number* 命令清除用户所在接口下的已学到的攻击者 ARP 表项。
- 如果配置的防欺骗模式为 **send-ack**，请执行步骤 2。
- 如果配置的防欺骗模式为 **fixed-mac**，请执行步骤 3。
- 如果配置的防欺骗模式是 **fixed-all**，请直接执行步骤 4。

步骤 2 **send-ack** 模式下，执行以下子步骤继续排查。

1. 通过端口镜像抓取接入用户的接口上的报文，查看是否有对应的 ARP 交互过程。如果 AR2200-S 没有发出 ARP 请求，请直接执行步骤 4。
2. 如果 AR2200-S 发出了 ARP 请求，但没有收到用户的 ARP 应答，检查设备和用户之间网络连接是否正常。
3. 如果收到用户的 ARP 应答，执行 **display cpu-defend statistics packet-type arp-reply** 命令检查 ARP Reply 报文是否被丢弃。如果 ARP Reply 报文的“Drop”计数不断增加，可能是被 CPCAR 机制丢弃了。可以通过 **packet-type** 命令适当放大速率限制值。
4. 如果执行完以上步骤后故障仍未排除，请执行步骤 4。

步骤 3 执行命令 **display arp all | include** *ip-address* 查看用户的 ARP 表项中哪些信息被修改。

如果是接口或 VLAN 信息被修改，在 **fixed-mac** 模式下认为是正常现象；如果是 MAC 被修改，则执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.2

相关日志

无

10.2.2 网关地址被仿冒的定位思路

常见原因

本类故障的常见原因主要包括：

版权所有 © 华为技术有限公司

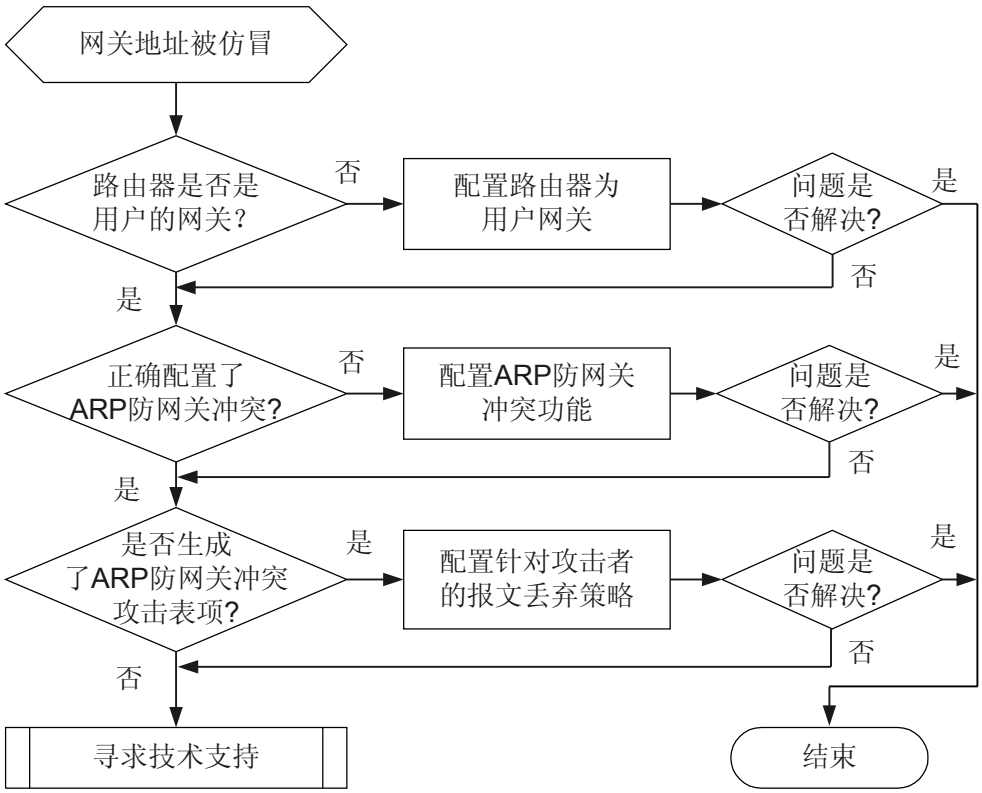
- 攻击者冒充网关发送免费 ARP 报文给用户，用户修改网关地址
- 攻击者冒充网关发送 ICMP 不可达攻击报文或者 ICMP 重定向报文给用户

故障诊断流程

攻击者仿冒网关地址，在局域网内部发送源 IP 地址是网关地址的免费 ARP 报文。局域网内部的主机接收到该报文后，会修改自己原来的网关地址为攻击者的地址，最终局域网内部所有主机无法访问网络。

详细处理流程如图 10-6 所示。

图 10-6 网关地址被仿冒故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 AR2200-S 设备是否为用户网关。如果网关不在 AR2200-S 上，配置了防网关冲突也无法生效。

有两种方法可以判断网关地址是否在 AR2200-S 上。

- 执行命令 **display arp**，查看网关地址对应的表项类型。

版权所有 © 华为技术有限公司

如果 **TYPE** 为 **I-**，表示接口本身的表项地址。

```
<Huawei> display arp
IP ADDRESS    MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                        VLAN/CEVLAN
------------------------------------------------------------------------------
1.1.1.1       0022-0033-0044            I -         Vlanif10
```

- 执行命令 **display ip routing-table** *ip-address*（用户网关地址），查看是否有路由。

  如果以下命令输出信息中没有针对网关地址的路由，则说明用户网关不在 AR2200-S 上。

```
<Huawei> display ip routing-table 1.1.1.1（用户网关地址）
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

1.1.1.1/24          Direct 0    0           D   127.0.0.1       Loopback0
```

步骤 2 执行命令 **display arp anti-attack configuration gateway-duplicate** 查看 ARP 防网关冲突功能是否使能。

如果没有使能 ARP 防网关冲突功能，则执行命令 **arp anti-attack gateway-duplicate enable** 使能该功能。

步骤 3 执行 **display current-configuration** 命令查看 AR2200-S 是否使能发送免费 ARP 报文功能。

- 当 AR2200-S 作为网关时，在 AR2200-S 上使能主动发送免费 ARP 报文的功能，使用户可以定时更新网关的 ARP 表项。使能方法为执行命令 **arp gratuitous-arp send enable**，此命令可以在系统视图或 VLANIF 视图下执行。
- 缺省情况下，使能主动发送免费 ARP 报文功能后，AR2200-S 每隔 90 秒发送一次免费 ARP 报文。如果用户希望自定义间隔时间，可以使用 **arp gratuitous-arp send interval** 命令进行设置。
- 如果发送免费 ARP 报文功能已使能，请执行步骤 4。

步骤 4 执行命令 **display arp anti-attack gateway-duplicate item** 查看防网关冲突攻击表项。

- 如果命令显示信息中有内容，表示攻击者的 IP、MAC、源接口等信息已被记录下来。可以根据该表项的内容配置对该用户的报文处理策略。方法有配置黑名单或黑洞 MAC 丢弃用户的报文。
- 如果命令显示信息为空，表示没有攻击者的表项，请执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.1

版权所有 © 华为技术有限公司

相关日志

无

10.2.3 ARP 报文攻击导致用户流量中断的定位思路

常见原因

本类故障的常见原因主要包括：

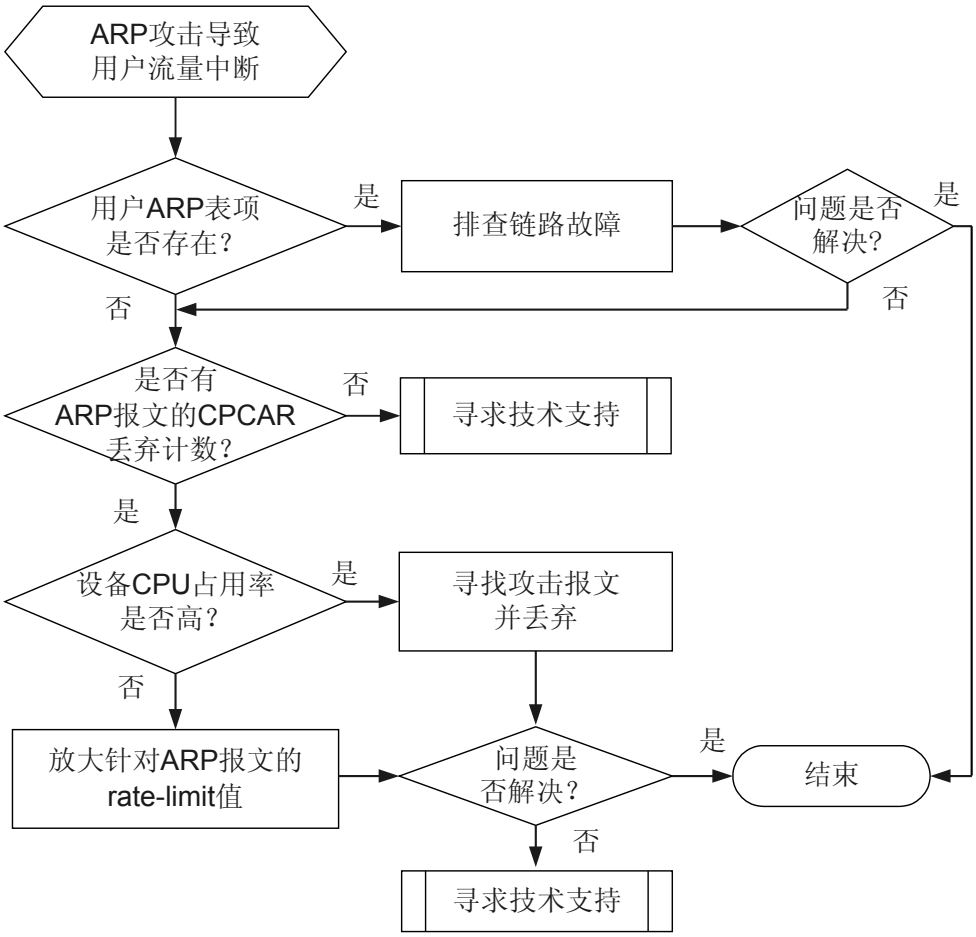
- 攻击者发送大量 ARP 报文，导致目的网段的负担加重。这些 ARP 报文还会送到 AR2200-S 的 CPU 增加了 CPU 的负担，同时有可能导致合法用户流量中断，形成拒绝服务攻击。

故障诊断流程

进入 AR2200-S 的 ARP 报文在上送 CPU 时有 CPCAR 机制进行限速。如果攻击者发送大量伪 ARP 报文，与合法用户的 ARP 报文共享 CPCAR 限制的带宽，就会导致合法的 ARP 报文被丢弃，从而导致用户流量中断。

详细处理流程如图 10-7 所示。

图 10-7 ARP 报文攻击导致用户流量中断故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

ARP 攻击报文包括 ARP Request 报文和 ARP Reply 报文，以下步骤中以 ARP Request 报文为例。针对 ARP Reply 的处理方法为把以下命令中涉及到的 **arp-request** 参数改为 **arp-reply** 即可。

操作步骤

步骤 1 执行命令 **display arp** 查看用户的 ARP 表项是否存在。

- 如果 ARP 表项还在，表明学到了用户的 ARP 表项，用户流量中断可能是用户的连接闪断。检查并排除链路问题。
- 如果没有用户表项，执行步骤 2。

步骤 2 执行命令 **display cpu-defend statistics packet-type arp-request** 查看 ARP Request 报文的“Drop”计数是否增长。

- 如果计数为 0，设备没有丢弃 ARP Request 报文。请执行步骤 8。
- 如果有计数，表示设备收到的 ARP Request 报文由于超过了 CPCAR 的速率限制而被丢弃。执行步骤 3。

步骤 3 执行命令 **display cpu-usage**，查看主用主控板的 CPU 占用率信息。

- 如果 CPU 占用率正常，而 ARP Request 报文被丢弃，可能是 CPCAR 限制值偏小。执行步骤 4。
- 如果 CPU 占用率较高，可能是 ARP 攻击报文被丢弃。请执行步骤 5。

步骤 4 执行命令 **packet-type** 适当放大针对 ARP Request 报文的 CPCAR 的限制值。

packet-type 命令应该在防攻击策略视图下执行，并应用该防攻击策略才能生效。

步骤 5 在 AR2200-S 与用户连接的接口上抓取报文，分析 ARP Request 报文的源地址，找出攻击者。

如果同一个源地址出现在很多 ARP Request 报文中，则 AR2200-S 认为该地址就是攻击源。可以通过配置黑名单或黑洞 MAC 对其报文进行丢弃处理。

步骤 6 在 AR2200-S 系统视图下执行命令 **arp speed-limit source-ip**，配置 ARP 报文源抑制速率。

缺省情况下，ARP 报文按源 IP 地址抑制功能使能，抑制速率为 5pps。

步骤 7 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

版权所有 © 华为技术有限公司

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.3
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.4
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.5
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.6
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.11

相关日志

无

10.2.4 IP 扫描攻击的定位思路

常见原因

本类故障的常见原因主要包括：

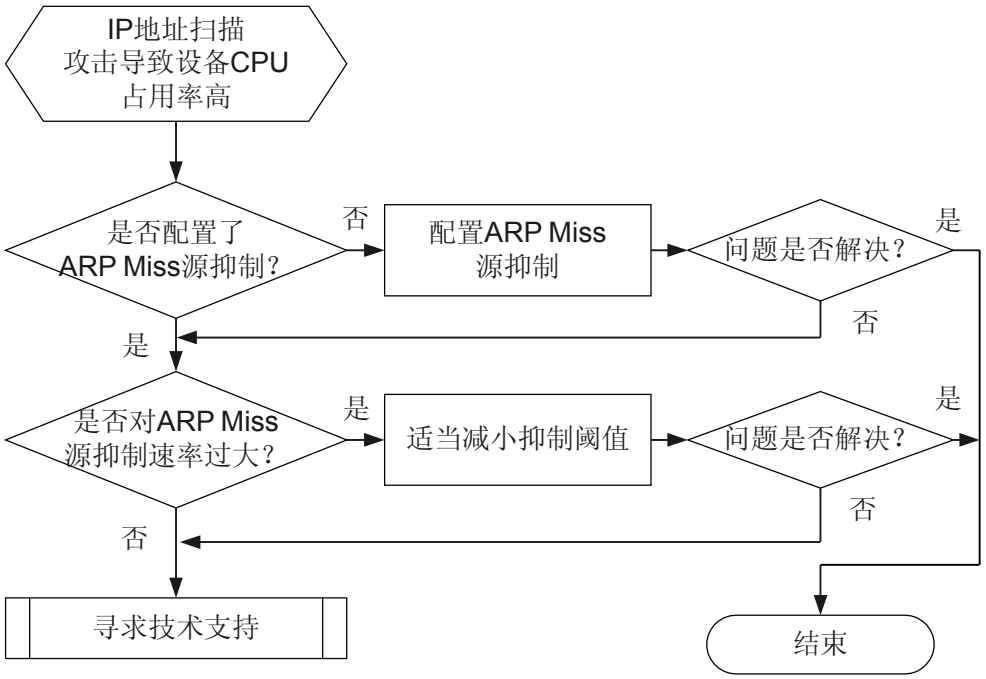
- 攻击者发送大量目的不可达报文，报文上送到 AR2200-S 的 CPU，触发 ARP Miss 消息，同时向网络上发送 ARP 请求进行 ARP 学习，消耗 CPU 资源。

故障诊断流程

AR2200-S 短期内收到太多目的地址不可达的报文，报文上送 CPU，触发 ARP Miss 消息，同时发送 ARP 请求进行 ARP 学习，消耗 CPU 资源。

详细处理流程如图 10-8 所示。

图 10-8 IP 地址扫描攻击故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 在 AR2200-S 上执行命令 **display cpu-usage**，查看单板的 CPU 占用率信息。

名为 **ARP** 的任务指的是 ARP 报文处理任务。

步骤 2 执行命令 **display arp** 查看 ARP 学习是否正常。

ARP 表项中 MAC 地址为 **Incomplete**，表示 ARP 学习失败。

```
<Huawei> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE    VPN-INSTANCE
                                          VLAN/CEVLAN
------------------------------------------------------------------------------
10.10.10.12     0018-82d2-0e08            I -         Vlanif10
10.10.10.13     Incomplete      0         D-0         Vlanif20
                                          3004/-
10.10.10.14     Incomplete      0         D-0         Eth2/0/0
                                          3004/-
20.20.20.33     000c-76bd-43d6            I -         Eth2/0/0
20.20.20.55     0013-7227-842f  17        D-0         Eth2/0/0
...                                       3003/-
```

ARP 学习失败的原因有多种，如 ARP 请求未发出去，或发送出去在网络上丢掉了，或未收到 ARP 应答。如果步骤 1 中已查出 **ARP** 任务的 CPU 占用率较高，ARP 学习失败常见的原因是 ARP 请求报文发送失败。执行步骤 3。

步骤 3 在 AR2200-S 与用户连接的接口上抓取报文，分析 IP 报文的源 IP 地址。

步骤 4 在 AR2200-S 上执行命令 **display arp anti-attack configuration arpmiss-speed-limit** 查看 ARP Miss 源抑制配置信息。

- 如果配置了针对指定 IP 地址的 ARP Miss 源抑制，判断该 IP 是否与 IP 报文的源 IP 地址一致；如果不一致则抑制速率就是未指定 IP 地址的配置速率。
- 缺省情况下，ARP Miss 源抑制功能是使能的，抑制速率为 5pps，即每秒 5 个 ARP Miss 消息。超过该速率，则对指定 IP 地址发送来的报文做丢弃处理。可以在系统视图下使用 **arp-miss speed-limit source-ip** 命令修改速率限制值。

步骤 5 在 AR2200-S 上执行命令 **display arp anti-attack configuration arpmiss-rate-limit** 查看 ARP Miss 速率抑制配置信息。

- 如果系统在一定时间内不断上报 ARP Miss 消息，使得设备由于忙于发送广播 ARP 请求而性能下降。ARP Miss 消息的抑制功能是对一定时间内上报的 ARP Miss 消息进行统计，并将超过限速值的 ARP Miss 消息丢弃的过程。
- 缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。可以在系统视图下执行命令 **arp-miss anti-attack rate-limit** 命令修改 ARP Miss 消息的限速时间和限速值。

步骤 6 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

版权所有 © 华为技术有限公司

- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.165.2.2.2.8
- 1.3.6.1.4.1.2011.5.25.165.2.2.2.12

相关日志

无

10.2.5 ARP 学习失败的定位思路

常见原因

ARP 学习失败，有以下几种可能（假设 AR2200-S 发送 ARP 请求）：

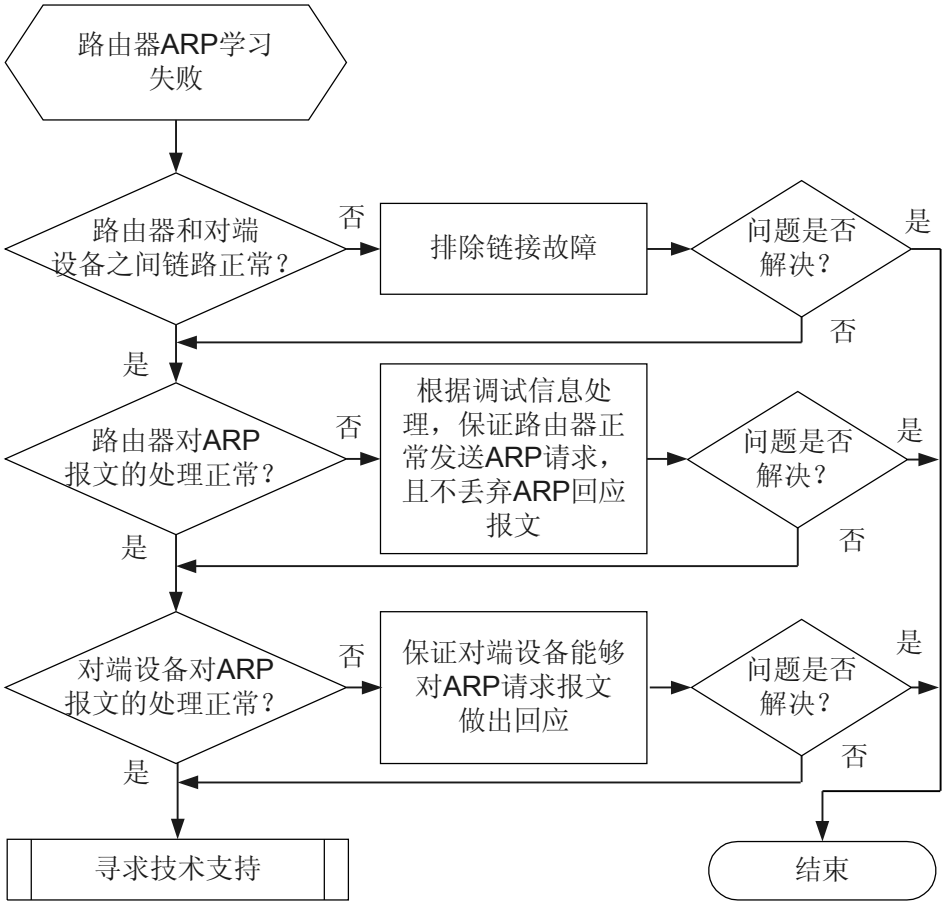
可能情况	可能原因
ARP 请求报文没有发出去	AR2200-S 短期内大量 ARP Miss 消息触发太多 ARP 请求，来不及发送出去
ARP 请求报文没有到达对方，在网络上被丢弃了	传输链路问题
ARP 请求报文到了对方设备，但是被对方设备丢弃了	对方设备受到攻击，收到大量 ARP 报文，报文被限速机制丢掉
对方的响应报文没有达到 AR2200-S	传输链路问题
对方的响应报文到达 AR2200-S 但是没有送到 CPU	被 AR2200-S 的 CPCAR 机制或 ARP 限速丢弃
对方响应报文到达 AR2200-S 的 CPU，但是被丢弃了	AR2200-S 的 ARP 处理模块出错

故障诊断流程

详细处理流程如图 10-9 所示。

版权所有 © 华为技术有限公司

图 10-9 ARP 学习失败故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 AR2200-S 和对端设备之间的链路是否正常。

- 可以通过 **ping** 命令检查两端的路由连通性。如果 ping 不通，请先解决路由的故障。
- 可以通过流量统计查看设备是否有丢包，如果设备不支持流量统计，可以通过上下互 ping 来测试。如果有丢包，请先排除设备转发的故障。

步骤 2 检查 AR2200-S 的 ARP 处理是否正常。

用户视图下使用命令 **debugging arp packet interface** *interface-type interface-number* 打开 ARP 报文调试开关，查看设备是否发出 ARP 请求报文、是否收到 ARP 回应报文。

说明

调试信息的“operation”字段表示协议类型：1 为 ARP 请求；2 为 ARP 响应。

- 如果没有发送过 ARP 请求报文，请参考 **10.2.4 IP 扫描攻击的定位思路**进行处理。

版权所有 © 华为技术有限公司

- 如果没有收到 ARP 回应报文，检查是否由于 CPCAR 机制丢弃了 ARP 回应报文。请参考步骤 3。
- 如果收到了 ARP 回应报文，请执行步骤 5。

步骤 3 检查 ARP 回应报文是否被丢弃。

- 执行命令 **display cpu-defend statistics packet-type arp-reply** 查看 ARP Reply 报文的“Drop”计数是否增长。

  如果计数一直增长，执行命令 **packet-type** 适当放大针对 ARP Reply 报文的 CPCAR 的限制值。
- 系统视图或接口视图下执行命令 **display this** 查看是否配置了 ARP 报文限速。

  如果配置了 ARP 报文限速功能“arp anti-attack rate-limit enable”，而 ARP 报文速率很大，则有可能被丢弃。使用命令 **arp anti-attack rate-limit** 可以修改速率抑制大小。

步骤 4 检查对端设备的 ARP 处理是否正常。

检查对端设备是否收到了 ARP 请求报文，如果收到是否响应了请求，是否发出 ARP 回应报文。

如果对端设备是华为设备，可以参考步骤 2 的描述；如果是其他厂商设备，请参考相应的操作手册。

步骤 5 如果故障依然存在，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.3 NAC 故障处理

10.3.1 802.1x 认证失败的定位思路

常见原因

本类故障的常见原因主要包括：

- 配置遗漏或配置错误（包括 802.1x 的配置，以及 AAA 方面的域、认证服务器、认证模板等配置）

版权所有 © 华为技术有限公司

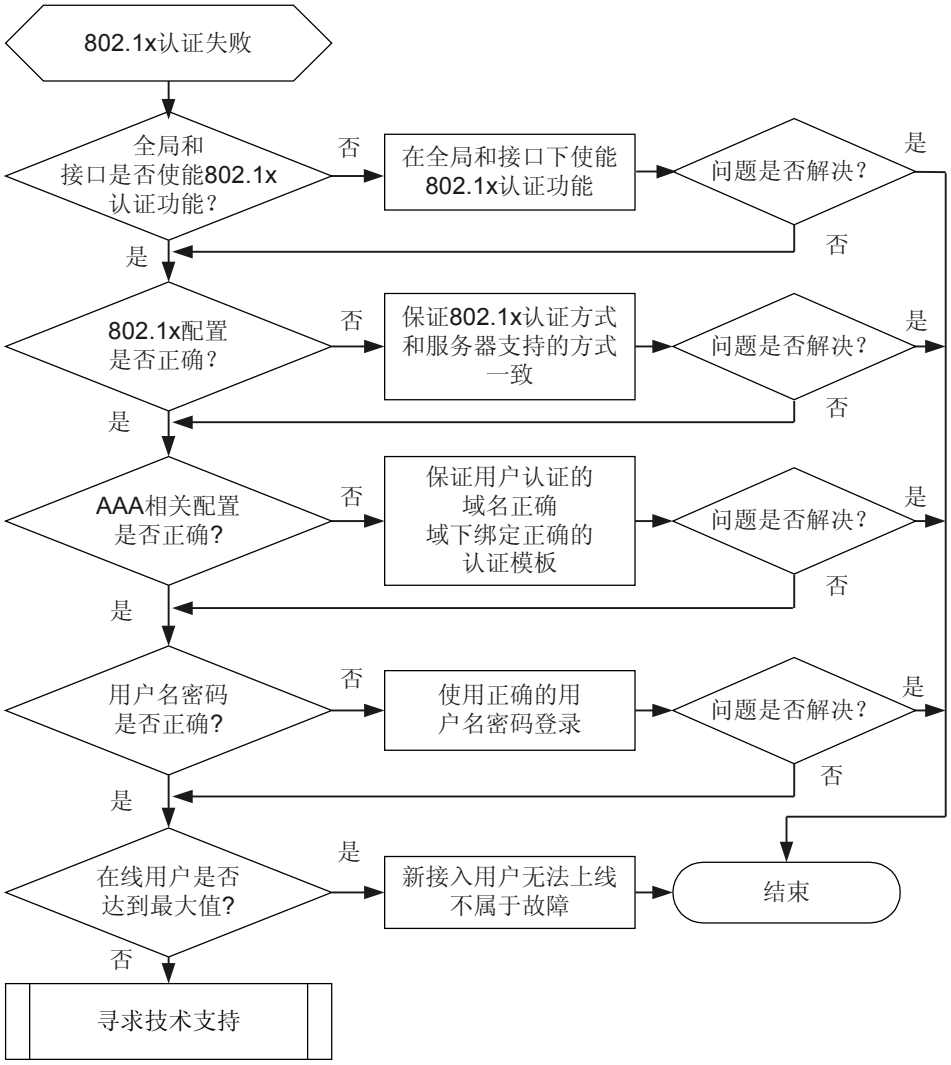
- 用户登录的用户名和密码不正确
- 上线的用户数已达到最大数量

故障诊断流程

配置接入用户使用 802.1x 认证，用户认证失败。

详细处理流程如图 10-10 所示。

图 10-10 802.1x 认证失败故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查 AR2200-S 是否使能 802.1x 认证功能。

使用命令 **display dot1x** 检查全局和接口下是否都使能了 802.1x 认证功能。如果没有 **Global 802.1x is enabled** 或 **802.1x protocol is enabled**，则 802.1x 认证功能未使能，需要执行 **dot1x enable** 命令使能。

注意

接口下 802.1x 认证和 MAC 地址认证有配置冲突关系，当接口下配置了 MAC 认证时，会有提示且不允许配置 802.1x 认证。

步骤 2 检查 802.1x 的配置是否正确。

使用命令 **display dot1x** 可以查看当前 802.1x 的配置信息。

AR2200-S 对 802.1x 用户的认证方法，支持终结认证（PAP 和 CHAP）和中继认证（EAP）。使用命令 **dot1x authentication-method** 可以配置 802.1x 用户的认证方法。

- AR2200-S 上配置的认证方式，和认证服务器支持的认证方式要一致。
- 如果配置了 802.1x 用户的认证方式为 EAP 认证（Authentication method is EAP），则 AAA 的认证方式不能为本地认证。AAA 的检查，请执行步骤 3。
- 如果配置了 802.1x 用户的认证方式为 PAP 认证（Authentication method is PAP），需要关注客户端是否支持 PAP 认证。如果客户端不支持 PAP 认证，选择 CHAP 或 EAP 认证方式。

步骤 3 查看 AAA 相关配置是否正确。

1. 查看用户拨号的用户名是否包含域名。
   - 如果没有包含域名，则用户会到 default 域进行认证，查看 default 域下绑定的模板。
   - 如果用户名包含域名，则会根据域名找到指定的域进行认证（如果找不到域名，则认证失败），此时需要查看该域下绑定的模板。
2. 查看 AR2200-S 上用户的域使用的认证方案。
   - 如果是 RADIUS 认证或 HWTACACS 认证，到相应的认证服务器上检查是否创建了相应的用户名和密码。还需查看服务器上是否有用户动态授权信息。具体 AR2200-S 上 RADIUS 故障或 HWTACACS 故障的处理方法，请参见 **10.1.1 RADIUS 用户认证失败的定位思路**和 **10.1.2 HWTACACS 用户认证失败的定位思路**。和服务器相关的检查内容，请参考步骤 4。
   - 如果是本地认证，执行命令 **display local-user** 查看是否创建了本地用户。若没有，需执行命令 **local-user** 创建用户名和密码。
   - 如果是不需认证（none），请执行步骤 6。
3. 执行命令 **display accounting-scheme** 查看计费方案，如果配置了计费而认证服务器不支持计费功能，则用户也无法上线。这种情况可以通过在域下取消计费的配置，或者在计费方案视图下使用 **accounting start-fail online** 命令配置计费策略为计费失败保持在线来规避。

步骤 4 查看认证服务器的相关信息。

- 如果认证服务器上没有用户信息，需要为用户创建帐号。

版权所有 © 华为技术有限公司

- 如果认证服务器的用户属性包括 VLAN 授权信息，而 VLAN 在 AR2200-S 上未创建，会导致 VLAN 授权失败，用户授权不成功。需要创建相应的 VLAN。
- 如果认证服务器的用户属性包括 ACL 授权信息（以 ACL 编号下发或直接下发 ACL 内容），而 ACL 在 AR2200-S 上未创建，或 ACL 格式与 AR2200-S 的要求不一致，会导致 ACL 授权失败，用户授权不成功。需要在 AR2200-S 上创建相应的 ACL。或者保证服务器下发的 ACL 格式符合 AR2200-S 对 ACL 授权格式的要求。

  说明

  AR2200-S 对下发的用户属性 ACL 内容格式要求为
  acl *acl-num* **key1** *key-value1*... **keyN** *key-valueN* **permit**/**deny**
  只有 **display access-user user-id** 查看到用户 IP 地址已经记录到用户表项中，有“Dynamic ACL desc (Effective)”信息，才表示用户属性的 ACL 生效。

表 10-1 命令参数含义

内容	含义	内容	含义
acl	关键字，表示下发的是 ACL 内容	*acl-num*	ACL 编号，取值范围为 10000 到 10999
permit	表示允许访问	**deny**	表示拒绝访问
keyM(1≤M≤N)：	ACL 语句关键字，可以取值 src-ip（源 IP）、src-ipmask（源 IP 掩码）、tcp-srcport（源 TCP 端口号）等	*key-valueM*(1 < M < N)	与 ACL 关键字对应的关键值，可以为 IP、IP 地址掩码、端口号等

如果 AR2200-S 和认证服务器上的配置都正确，再从客户端去排查问题。请执行步骤 5。

步骤 5 与管理员确认用户拨号的用户名密码是否正确。

如果采用的是 RADIUS 远端认证，对于 CHAP/PAP 模式，可以使用 **test-aaa** 命令测试用户名和密码是否能快速通过 RADIUS 认证。

- 如果未通过，检查 RADIUS 服务器配置和 AR2200-S 上的 RADIUS 配置，保证配置正确。检查内容可以参考 **10.1.1 RADIUS 用户认证失败的定位思路**中的**故障处理步骤**。
- 如果通过，则需检查客户端选项设置或在客户端网卡上抓包看报文是否正确。保证客户端发出的报文正确。

如果用户名和密码没有问题，请执行步骤 6。

步骤 6 在 AR2200-S 执行命令 **display dot1x interface** *interface-type interface-number* 查看当前在线的 802.1x 用户数是否已达到最大值。

当接口接入的用户数达到最大数量时，AR2200-S 将不会再对之后接入的用户触发认证动作。

步骤 7 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

版权所有 © 华为技术有限公司

- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.40.4.2.1

相关日志

无

10.3.2 MAC 认证失败的定位思路

常见原因

本类故障的常见原因主要包括：

- 配置遗漏或配置错误（包括 MAC 认证的配置，以及 AAA 方面的域、认证服务器、认证模板等配置）
- 上线的用户数已达到最大数量

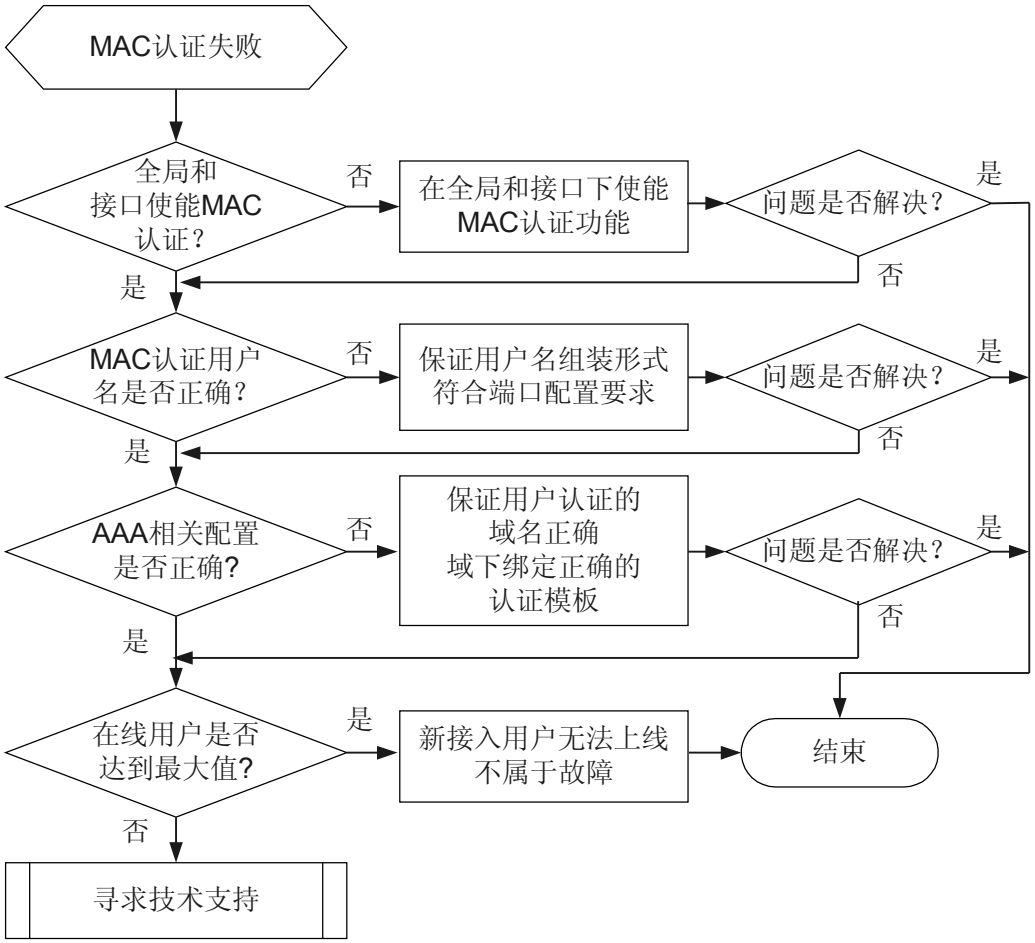
故障诊断流程

配置接入用户使用 MAC 地址认证，用户认证失败。

详细处理流程如**图 10-11** 所示。

版权所有 © 华为技术有限公司

图 10-11 MAC 地址认证失败故障诊断流程图



故障处理步骤

背景信息

MAC 认证不使用客户端拨号软件，认证所需要的用户名密码等信息通过配置和用户 MAC 来取得组装形成。在处理 MAC 认证失败的问题时，大体流程跟 802.1x 认证故障处理流程类似，主要关注 AR2200-S 上用户名配置跟认证服务器创建的用户名密码是否匹配，用户名中的域信息是否正确。

说明

请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。

操作步骤

步骤 1 检查 AR2200-S 是否使能 MAC 地址认证功能。

使用命令 **display mac-authen** 检查全局和接口下是否都使能了 MAC 地址认证功能。如果没有 **MAC address authentication is enabled**，则 MAC 认证功能未使能，需要执行 **mac-authen** 命令使能。

版权所有 © 华为技术有限公司

注意

接口下 MAC 地址认证和 802.1x 认证有配置冲突关系，当接口下配置了 802.1x 认证时，会有提示且不允许配置 MAC 认证。

步骤 2 检查 MAC 地址认证用户名的配置是否正确。

执行 **display mac-authen** 可以查看当前 MAC 认证的配置信息。

MAC 认证支持两种方式组装用户名：固定用户名形式和 MAC 地址形式。

- 如果采用 MAC 地址用户名形式，AR2200-S 取接入终端的 MAC 地址作为用户名和密码上送服务器认证。认证的域取 **mac-authen domain** 命令配置的域，如果没有配置该命令，则取默认的 default 域为认证域。
- 如果采用固定格式用户名，且在用户名中指定了域，则采用用户自带的认证域。如果没有在用户名中带上认证域，则默认取 default 域为认证域。

说明

MAC 地址的格式有两种：带分隔符“-”和不带分隔符。缺省情况下为不带分隔符，可以通过 **mac-authen username macaddress format with-hyphen** 命令设置输入 MAC 地址时带分隔符。在认证过程中输入用户名时，MAC 地址格式要和 AR2200-S 上的配置保持一致。

根据用户名中的域信息，到相应域下查看绑定的认证服务器模板和 AAA 方案是否正确。请参考步骤 3。

步骤 3 查看 AAA 相关配置是否正确。

1. 查看域下绑定的认证服务器模板是否正确；该模板的认证服务器的地址、端口是否正确。查看服务器模板中对用户名格式的处理和共享密钥是否和服务器上的配置一致。
2. 查看 AR2200-S 上用户的域使用的认证方案。
   - 如果是 RADIUS 认证或 HWTACACS 认证，到相应的认证服务器上检查是否创建了相应的用户名和密码。还需查看服务器上是否有用户动态授权信息。具体 AR2200-S 上 RADIUS 故障或 HWTACACS 故障的处理方法，请参见 **10.1.1 RADIUS 用户认证失败的定位思路**和 **10.1.2 HWTACACS 用户认证失败的定位思路**。和服务器相关的检查内容，请参考步骤 4。
   - 如果是本地认证，执行命令 **display local-user** 查看是否创建了本地用户。若没有，需执行命令 **local-user** 创建用户名和密码。
   - 如果是不需认证（none），请执行步骤 5。
3. 执行命令 **display accounting-scheme** 查看计费方案，如果配置了计费而认证服务器不支持计费功能，则用户会上线后立即下线。这种情况可以通过在域下取消计费的配置，或者在计费方案视图下使用 **accounting start-fail online** 命令配置计费策略为计费失败保持在线来规避。

步骤 4 查看认证服务器的相关信息。

- 如果认证服务器上没有用户信息，需要为用户创建帐号。
- 如果认证服务器的用户属性包括 VLAN 授权信息，而 VLAN 在 AR2200-S 上未创建，会导致 VLAN 授权失败，用户授权不成功。需要创建相应的 VLAN。
- 如果认证服务器的用户属性包括 ACL 授权信息（以 ACL 编号下发或直接下发 ACL 内容），而 ACL 在 AR2200-S 上未创建，或 ACL 格式与 AR2200-S 的要求不一致，会导致 ACL 授权失败，用户授权不成功。需要在 AR2200-S 上创建相应的 ACL。或者保证服务器下发的 ACL 格式符合 AR2200-S 对 ACL 授权格式的要求。

版权所有 © 华为技术有限公司

说明

AR2200-S 对下发的用户属性 ACL 内容格式要求为
acl *acl-num* **key1** *key-value1*... **keyN** *key-valueN* **permit**/**deny**
只有 **display access-user user-id** 查看到用户 IP 地址已经记录到用户表项中，有“Dynamic ACL desc (Effective)”信息，才表示用户属性的 ACL 生效。

表 10-2 命令参数含义

内容	含义	内容	含义
acl	关键字，表示下发的是 ACL 内容	*acl-num*	ACL 编号，取值范围为 10000 到 10999
permit	表示允许访问	**deny**	表示拒绝访问
keyM(1≤M≤N)：	ACL 语句关键字，可以取值 src-ip（源 IP）、src-ipmask（源 IP 掩码）、tcp-srcport（源 TCP 端口号）等	*key-valueM*(1 ＜ M ＜ N)	与 ACL 关键字对应的关键值，可以为 IP、IP 地址掩码、端口号等

如果 AR2200-S 和认证服务器上的配置都正确，请执行步骤 5。

步骤 5 在 AR2200-S 执行命令 **display mac-authen interface** *interface-type interface-number* 查看当前在线的 MAC 认证用户数是否已达到最大值。

当接口接入的用户数达到最大数量时，AR2200-S 将不会再对之后接入的用户触发认证动作。

步骤 6 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

- 1.3.6.1.4.1.2011.5.25.171.2.1

相关日志

无

10.3.3 MAC 旁路认证失败的定位思路

使用 MAC 旁路认证，接入终端首先以 802.1x 开始认证，由 ARP/DHCP 报文触发 AR2200-S 发起 802.1x 认证，如果终端长时间内（30 秒）没有回应 802.1x 报文，则以终端的 MAC 地址为认证信息，同时作为用户名和密码上送认证服务器进行认证。

版权所有 © 华为技术有限公司

MAC 旁路认证，指当终端 802.1x 认证失败后自动转入 MAC 认证。接口下 MAC 地址认证和 802.1x 认证有配置冲突关系，当接口下配置了 802.1x 认证时，会有提示且不允许配置 MAC 认证。但是 **dot1x mac-bypass** 命令相当于打开了 MAC 认证功能。旁路认证取终端的 MAC 地址作为用户名和密码，认证流程和 MAC 认证流程相同。MAC 旁路认证失败的处理流程和 MAC 认证失败的处理流程类似，请参见 **10.3.2 MAC 认证失败的定位思路**。

10.3.4 Web 认证失败的定位思路

常见原因

本类故障的常见原因主要包括：

- 配置遗漏或配置错误（包括 Web 认证的配置，以及 AAA 方面的域、认证服务器、认证模板等配置）
- Web 认证服务器不可达或不可用
- 用户登录的用户名和密码不正确

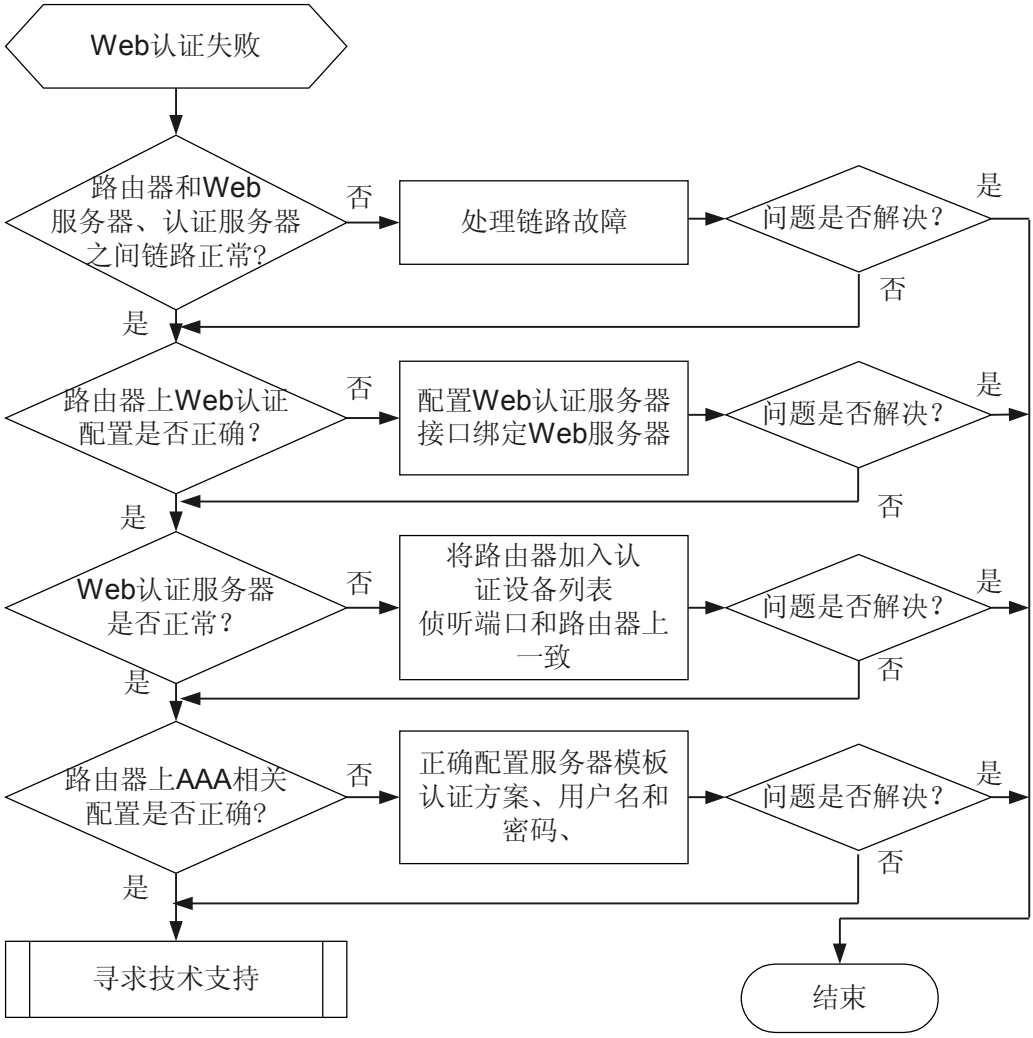
故障诊断流程

配置接入用户使用 Web 认证，用户认证失败。

详细处理流程如**图 10-12** 所示。

版权所有 © 华为技术有限公司

图 10-12 Web 认证失败故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 通过 **ping** 检查 AR2200-S 和 Web 认证服务器之间、AR2200-S 和 RADIUS 或 HWTACACS 服务器之间的链路是否有故障。

- 如果 ping 不通，请先根据 **7.1.1 Ping 不通问题的定位思路**排除链路的故障。
- 如果能 ping 通，请执行步骤 2。

步骤 2 检查 AR2200-S 上 Web 认证的配置是否正确。

- 执行命令 **display web-auth-server configuration** 查看是否配置了 Web 认证服务器。如果没有配置，在系统视图下执行命令 **web-auth-server（系统视图）**创建 Web 认证服务器名称，并在 web-auth-server 视图下执行 **server-ip** 命令配置服务器的 IP 地址。

版权所有 © 华为技术有限公司

在 web-auth-server 视图下还可以选择配置服务器端口 **port**、共享密钥 **shared-key** 和服务器 URL**url**。如果配置，要保证和服务器端的配置一致；如果不配，则默认端口号为 50100，共享密钥和 URL 为空。

- 在 VLANIF 接口视图下执行命令 **display this** 查看接口下是否绑定了 Web 认证服务器。如果没有绑定，在接口视图下执行命令 **web-auth-server（接口视图）**进行配置。
- 查看 **display web-auth-server configuration** 命令的显示信息中的侦听端口号（Listening port）是否和 Web 认证服务器上的一致。Web 认证服务器的检查，请执行步骤 3。

步骤 3 检查 Web 认证服务器配置是否正确。

- 在 Web 认证服务器上查看是否将 AR2200-S 加入了认证设备列表。
- 查看 Web 认证服务器和 AR2200-S 交互 Portal 报文的端口号，是否与 AR2200-S 上的配置一致。
- 在 Web 认证服务器上查看用户的 IP 地址是否在 AR2200-S 的 IP 地址组中。

保证 Web 认证服务器将 AR2200-S 加入了认证设备列表，侦听端口和 AR2200-S 的配置一致，且用户的 IP 地址在 AR2200-S 的地址组中。

步骤 4 查看 AAA 相关配置是否正确。

1. 查看域下绑定的认证服务器模板是否正确；该模板的认证服务器的地址、端口是否正确。查看服务器模板中对用户名格式的处理和共享密钥是否和服务器上的配置一致。
2. 查看 AR2200-S 上用户的域使用的认证方案。
   - 如果是 RADIUS 认证或 HWTACACS 认证，到相应的认证服务器上检查是否创建了相应的用户名和密码。确保用户使用正确的用户名和密码登录。具体 AR2200-S 上 RADIUS 故障或 HWTACACS 故障的处理方法，请参见 **10.1.1 RADIUS 用户认证失败的定位思路**和 **10.1.2 HWTACACS 用户认证失败的定位思路**。
   - 如果是本地认证，执行命令 **display local-user** 查看是否创建了本地用户。若没有，需执行命令 **local-user** 创建用户名和密码。
   - 如果是不需认证（none），请执行步骤 5。
3. 执行命令 **display accounting-scheme** 查看计费方案，如果配置了计费而认证服务器不支持计费功能，则用户会上线后立即下线。这种情况可以通过在域下取消计费的配置，或者在计费方案视图下使用 **accounting start-fail online** 命令配置计费策略为计费失败保持在线来规避。

步骤 5 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

版权所有 © 华为技术有限公司

相关日志

无

10.4 DHCP Snooping 故障处理

10.4.1 DHCP Snooping 导致用户无法上线的定位思路

常见原因

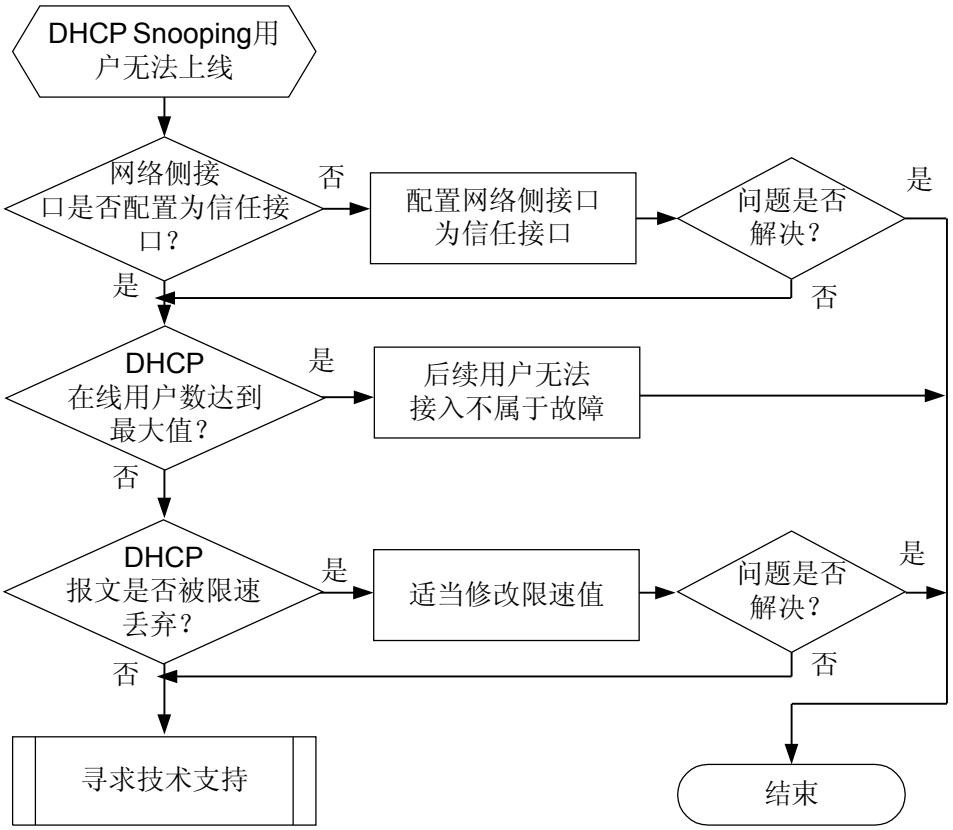
本类故障的常见原因主要包括：

- 连接 DHCP Server 的网络侧接口未配置为“信任”状态
- 用户侧接口下 DHCP 用户数达到定义的最大值
- DHCP 报文过多，超过限速，导致新用户的 DHCP 报文被丢弃

故障诊断流程

配置 DHCP Snooping 后发现用户无法上线，详细处理流程如图 10-13 所示。

图 10-13 配置 DHCP Snooping 后用户无法上线故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 查看信任接口是否配置错误。

执行命令 **display dhcp snooping global** 查看 DHCP Snooping 在哪个 VLAN 下、哪些接口下使能。

- 执行命令 **display dhcp snooping interface** 查看网络侧接口下是否有“dhcp snooping trusted”信息。
- 在 VLAN 视图下执行命令 **display this**，查看是否有“dhcp snooping trusted interface xxx”信息。

“trusted”是接口信任状态的标识。接口使能了 DHCP Snooping 功能后，默认都是“不信任”状态。对网络侧报文：AR2200-S 只处理信任接口收到的 DHCP Reply 报文，非信任接口收到 DHCP Reply 报文会丢弃；对用户侧报文：用户的请求报文进来以后，只会向信任接口转发。

- 连接 DHCP Server 的网络侧接口应该配置为“Trusted”。如果没有配置 Trusted，在接口视图下执行命令 **dhcp snooping trusted** 或在 VLAN 视图下执行命令 **dhcp snooping trusted interface** 配置接口为“信任”状态。
- 如果接口信任状态配置正确，请执行步骤 2。

步骤 2 查看 DHCP 上线用户数是否达到定义的最大值。

- 执行命令 **display dhcp snooping interface** 查看用户侧接口下是否有“dhcp snooping max-user-number xxx”信息。
- 在 VLAN 视图下执行命令 **display this**，查看是否有“dhcp snooping max-user-number xxx”信息。

以上的“max-user-number”是配置的 DHCP 最大用户数，如果没有该信息，则取默认值 1024 个。如果配置了则以配置值为准；如果两个视图下都配置了该参数，系统会取两者中的最小值来限制。

执行命令 **display dhcp snooping user-bind all** 查看当前 AR2200-S 使能 DHCP Snooping 功能的接口上一共生成多少 DHCP 用户动态绑定表项。如果已经达到配置的限制值，后续用户无法接入不属于故障。

如果 DHCP 上线用户数未达到配置的限制值，请执行步骤 3。

步骤 3 查看是否 DHCP 报文过多，超过限速值而被丢弃。

分别在接口视图、VLAN 视图、系统视图下执行命令 **display this** 查看是否配置了 DHCP 报文限速。如果没有“dhcp check dhcp-rate xx”信息，表示使用缺省的限速值 100。

DHCP 报文的限速在全局、接口和 VLAN 都可以配置，限速指的是在一定的时间内只允许规定数目的报文上送协议栈处理，超过速率规定的报文将被丢弃。如果在全局、接口、VLAN 都配置了限速，则取配置的最小值生效。如果 DHCP 报文的限速值较小，使用命令 **dhcp check dhcp-rate**（该命令可以在系统视图、接口视图、VLAN 视图下执行）适当增大限速值。

版权所有 © 华为技术有限公司

如果增大了限速值后故障仍未排除，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.5 防火墙故障处理

10.5.1 用户通过流量监测工具发现网络中存在大量的 SYN 报文

由于资源的限制，TCP/IP 栈的实现只能允许有限个 TCP 连接。

SYN Flood 攻击是指攻击者发送一个 SYN 报文，其源地址是伪造的、或者是一个不存在的地址，向服务器发起连接，服务器在收到报文后用 SYN-ACK 应答，而此应答发出去后，不会收到 ACK 报文，造成一个半连接。如果攻击者发送大量这样的报文，会在被攻击主机上产生大量的半连接，耗尽其资源，使正常的用户无法访问，直到半连接超时。

常见原因

本类故障的常见原因包括：

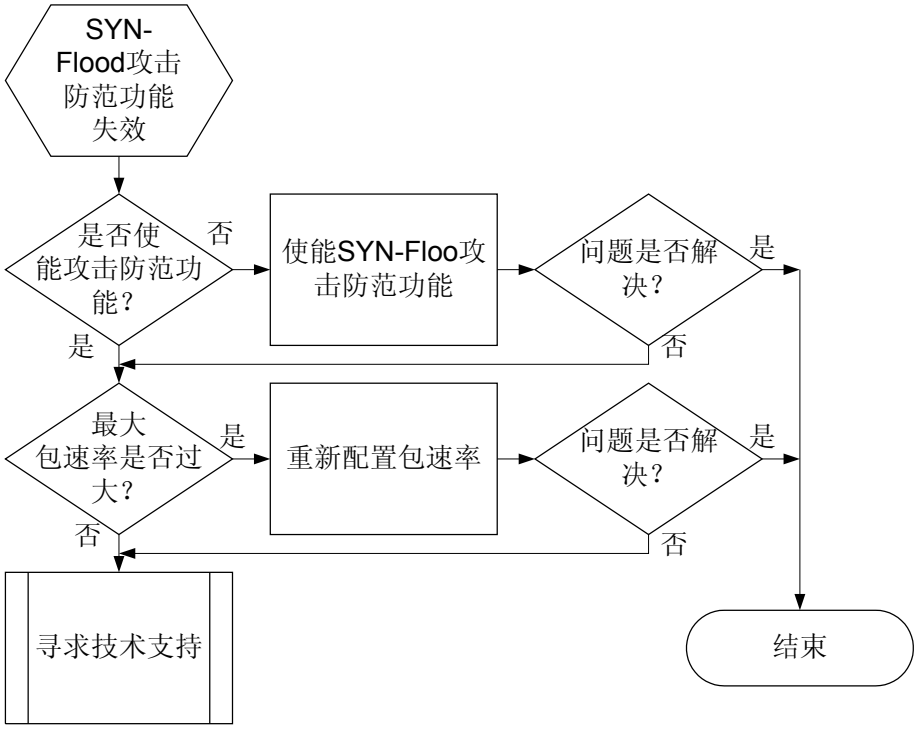
- 未使能 SYN Flood 攻击防范功能。
- 防火墙上配置的最大包速率阈值太大。

故障诊断流程

SYN Flood 攻击防范故障详细处理流程如图 10-14 所示。

版权所有 © 华为技术有限公司

图 10-14 SYN Flood 攻击防范故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 SYN Flood 攻击防范功能是否使能

执行 **display firewall defend flag** 命令，检查 SYN Flood 攻击防范功能是否使能。SYN Flood 对应的 Flag 的值如果为“Enable”，说明已经使能 SYN Flood 攻击防范功能。

如果 SYN Flood 攻击防范功能没有使能，请在系统视图下执行 **firewall defend syn-flood enable** 使能攻击防范功能。

如果 SYN Flood 攻击防范功能已经使能，请执行步骤 2。

步骤 2 检查配置的最大包速率阈值是否太大

执行 **display firewall defend syn-flood ip** 或者 **display firewall defend syn-flood zone** 命令检查用户配置基于 ip 的或者基于 zone 的最大包速率。

显示信息中“MR(pps)”表示最大包速率，即每秒内最多允许多少个目的 IP 地址相同的包通过。

说明

缺省情况下，最大包速率为 1000 pps。

版权所有 © 华为技术有限公司

- 如果需要配置或者修改最大包速率，请在系统视图下执行 **firewall defend syn-flood** 命令。
- 如果最大包速率配置正常，请执行步骤 3。

步骤 3 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

FIREWALL 1.3.6.1.4.1.2011.5.25.222.1.3.2 hwFwSecurityNotification

相关日志

无

10.6 ACL 故障处理

10.6.1 ACL 不起作用引起包过滤防火墙失效的定位思路

常见原因

本类故障的常见原因包括：

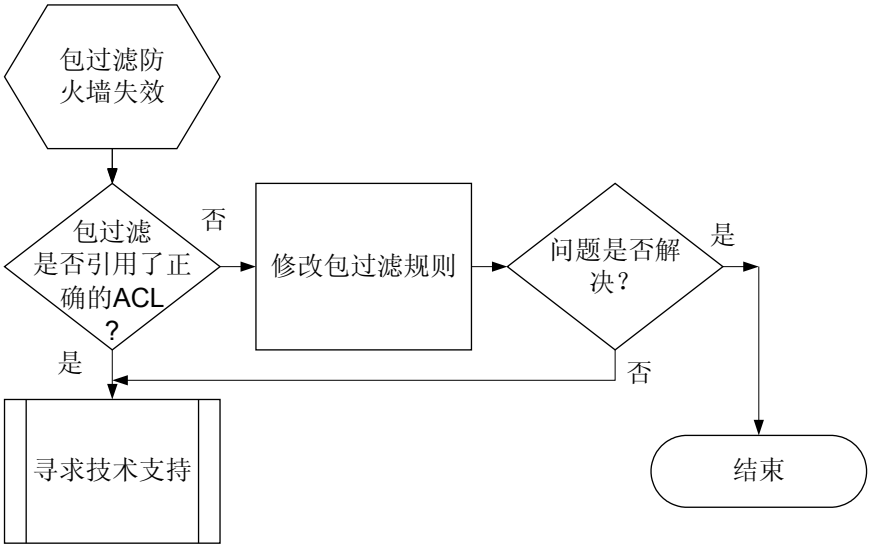
- 引用了错误的 ACL 编号
- ACL 的规则定义错误

故障诊断流程

故障详细处理流程如图 **10-15** 所示。

版权所有 © 华为技术有限公司

图 10-15 ACL 不起作用引起包过滤防火墙失效故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查包过渡引用的 ACL 是否配置正确

执行 **display firewall interzone** 可以检查包过滤引用的 ACL 序列号及应用方向。设备上可能存在多个 ACL，引用时需要注意引用到正确的 ACL。

- 如果引用的 ACL 编号错误或者 ACL 应用方向错误，请在安全域间视图下，执行 **undo packet-filter** { *acl-number* | **default** { **deny** | **permit** }} { **inbound** | **outbound** } 取消配置包过滤后，执行 **packet-filter** { *acl-number* | **default** { **deny** | **permit** }} { **inbound** | **outbound** } 命令重新配置 ACL 的应用方向。
- 如果引用的 ACL 编号正确，应用方向也正确，请执行 **display acl** 命令检查 ACL 的规则配置是否正确。如果规则配置错误，请修改 ACL 的配置规则。如果规则正确，请执行步骤 2。

步骤 2 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

版权所有 © 华为技术有限公司

相关日志

无

10.7 NAT 故障处理

10.7.1 NAT Outbound 故障现象：内网用户无法访问公网

常见原因

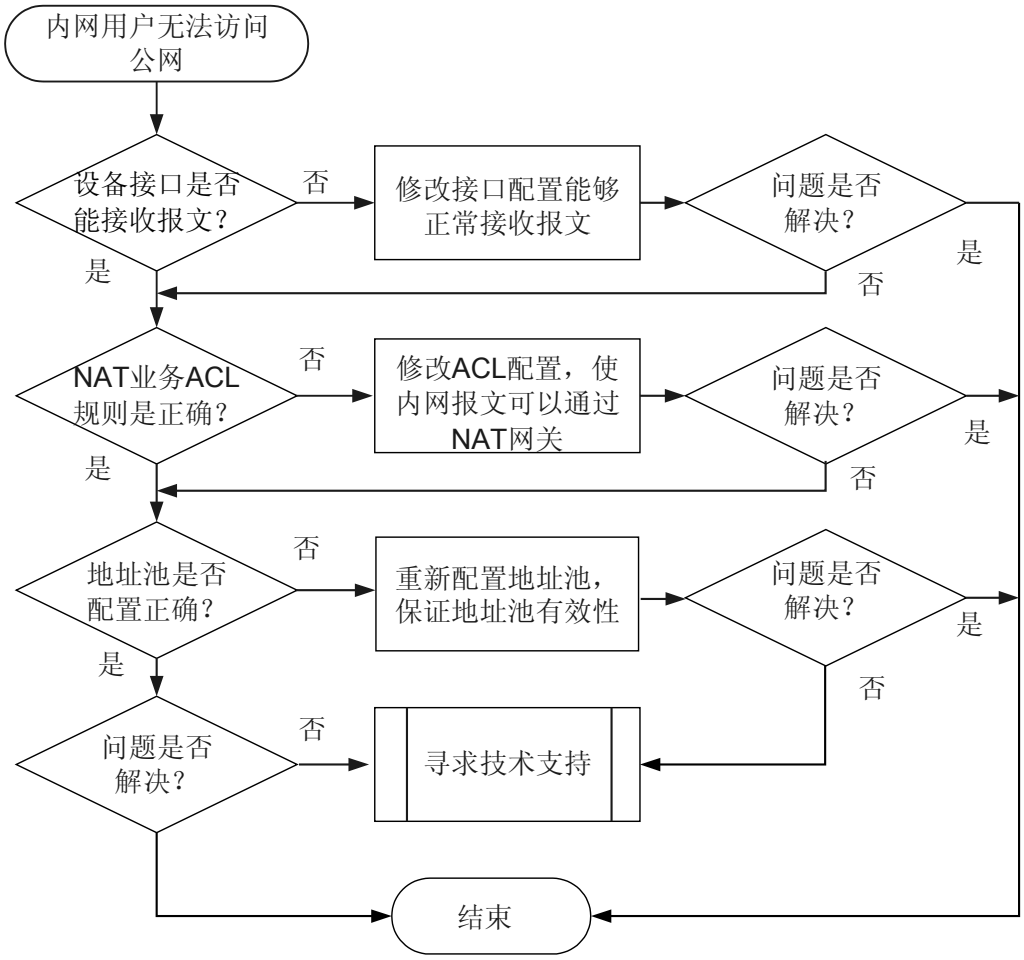
本类故障的常见原因包括：

- 用户访问公网的出、入接口状态 Down
- 未在访问公网的出接口上正确配置 NAT Outbound
- NAT Outbound 引用的 ACL 配置错误

故障诊断流程

详细处理流程，如图 10-16 所示。

图 10-16 NAT Outbond 故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 AR2200-S 的接口是否有报文进入

在 AR2200-S 上执行 **display interface interface-type** *interface-number* 命令，查看显示信息的 **Input** 字段值。

- 如果 **Input** 字段值为 0，表示 AR2200-S 没有报文进入，请排查接口的配置，保证接口能接收报文。
- 如果 **Input** 字段值不为 0，请执行步骤 2。

说明

AR2200-S 支持 GE,FE,Eth-Trunk 及子接口等多种接口。如果使用的是 Eth-Trunk 子接口，使用 **display interface eth-trunk** [*trunk-id* [*.subnumber*]] 命令查看接口是否有报文进入。

步骤 2 检查 NAT Outbound 绑定的 ACL 规则，是否允许 NAT 业务报文通过

在 AR2200-S 上执行命令 **display nat outbound**，查看出接口上是否正确配置了 NAT Outbound。

```
[Huawei]display nat outbound
  NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface                        Acl      Address-group/IP      Type
 ----------------------------------------------------------------------
 GigabitEthernet0/0/0            2000                     1    no-pat
 ----------------------------------------------------------------------
  Total : 1
```

由显示信息可知 NAT 出接口 GigabitEthernet0/0/0 上 NAT Outbound 关联的 ACL 号为 2000。

然后查看 ACL 2000 的规则配置是否正确。如果 ACL 2000 未配置正确的 IP 地址、端口号或协议类型，将导致报文无法正常出入网络。

使用命令 **display acl 2000** 查看当前 ACL 2000 关联的 NAT Outbound 配置。

```
[Huawei] display acl 2000
Advanced ACL2000, 1 rule
Acl's step is 5
rule 5 permit source 192.168.1.100 0
```

根据 ACL 规则可以看出，报文类型为 TCP，源地址为 192.168.1.100 的报文才能够匹配该 ACL 规则，进行 NAT 业务。

- 如果 ACL 匹配规则配置错误，请重新进行配置。
- 如果 ACL 匹配规则配置正确，故障仍然存在，请执行步骤 3。

步骤 3 检查地址池配置是否正确

在 AR2200-S 上执行命令 **display nat address-group**，查看出接口上 NAT Outbound 所绑定的地址池是否正确。

```
[Huawei] display nat address-group 1
NAT Address-Group Information:
```


版权所有 © 华为技术有限公司

```
-------------------------------------
Index   Start-address      End-address
-------------------------------------
1       110.0.0.100         110.0.0.110
-------------------------------------
Total : 1
```

针对 Easy IP 方式，需要在 AR2200-S 上执行命令 **display nat outbound**，查看 NAT 出接口上配置的 Easy IP 信息。

```
[Huawei] display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface                 Acl       Address-group/IP       Type
 ----------------------------------------------------------------------
 GigabitEthernet0/0/1      2000            30.30.30.1     easyip
 ----------------------------------------------------------------------
  Total : 1
```

由上述信息可以看到出接口 GigabitEthernet0/0/1 配置的是 Easy IP 方式，并且绑定的地址池是接口上发布的地址 30.30.30.1。如果 NAT 不通，需要确认：

- 绑定的 IP 地址是否是接口的 IP 地址，如果是则需要确认接口地址的有效性
- 绑定的地址是否是 VRRP 虚拟地址，如果是则首先确认接口地址是否存在，然后确认 VRRP 的状态是否为 Master 状态，可以在接口视图下执行 **display vrrp** 来查看该接口下的 VRRP 状态。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.7.2 NAT Server 故障现象：外网主机无法访问内网服务器

常见原因

本类故障的常见原因主要包括：

- 内网服务器上对应的应用层服务没有打开
- NAT Server 配在错误的接口上（比如，配置在出接口上，或其他不相关的接口上），正确应该配置在外网主机访问内网的入接口上

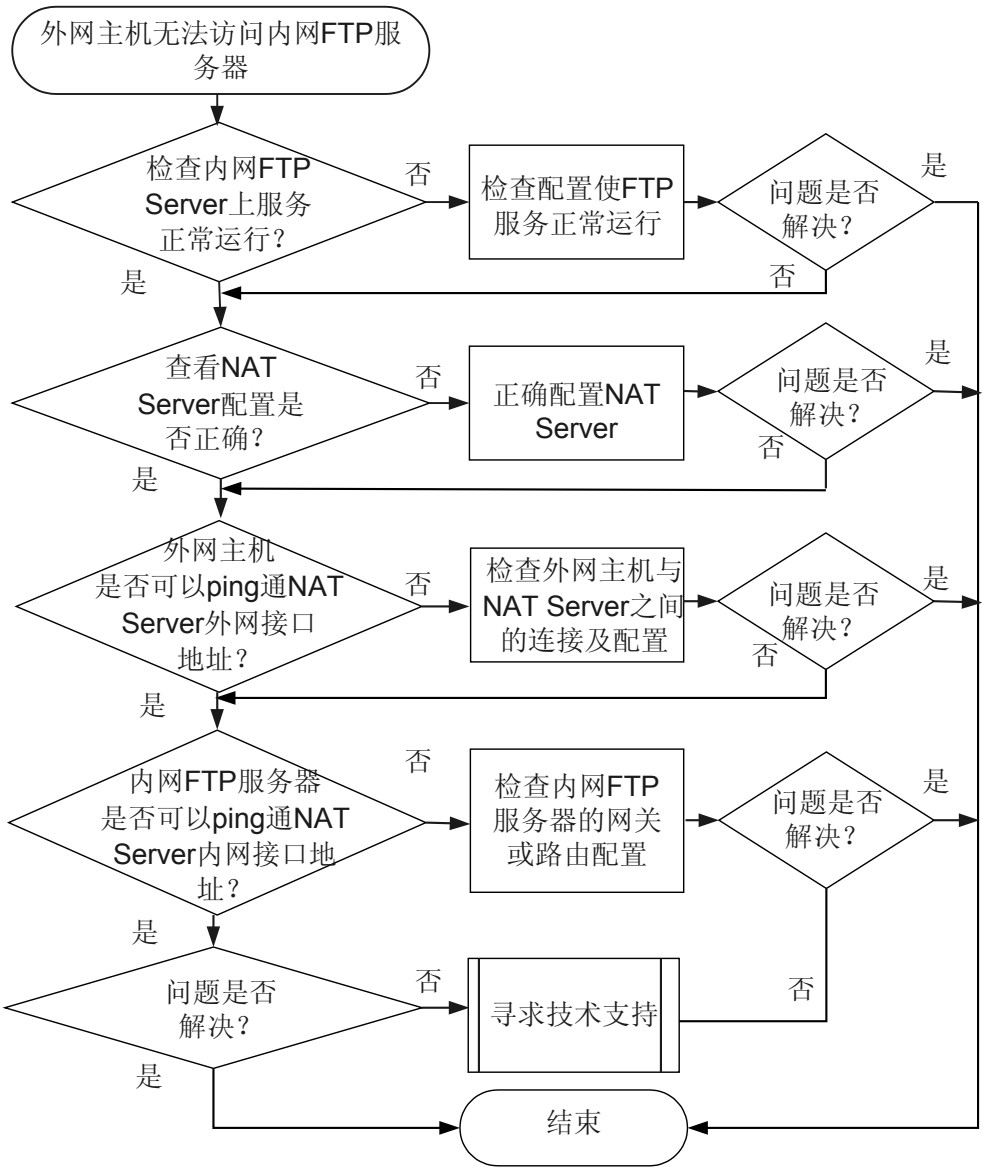
版权所有 © 华为技术有限公司

- NAT Server 配置错误（比如，配置的内部 Server 对应的公网、私网 IP 地址不对，私网端口和内部服务器打开的端口不一样）

故障诊断流程

详细处理流程，如图 10-17 所示。

图 10-17 NAT Server 故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查内网 NAT Server 上的应用服务正常

当从外网无法访问 NAT Server 所提供的服务时，先确认内网服务器上相应的服务（例如 HTTP Server，FTP Server 等）是否打开。可以从内网其他主机上尝试访问内网服务器，以确保相应服务正在运行。

- 如果内网 NAT Server 上的应用服务未正常运行，请打开相应服务。
- 如果内网 NAT Server 上的应用服务正常运行，故障仍然存在，请执行步骤 2。

步骤 2 检查 NAT Server 配置是否正确

在 AR2200-S 上执行命令 **display nat server**，查看 NAT Server 是否配置在正确的 NAT 接口上，是否配置了正确的协议、端口和地址信息。

```
[AR2200-S]display nat server
  Nat Server Information:
  Interface  : GigabitEthernet0/0/1
    Global IP/Port     : 202.10.10.10    21(ftp)
    Inside IP/Port     : 10.10.10.2       21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
  Total :    1
```

特别需要注意的是，被映射的内网地址和端口是否正确。某些服务传送报文数据时，会使用到多个端口（有些端口是随机产生的），例如 FTP 和 TFTP，因此为这些服务配置 NAT Server 时，应该把对端口的限制放开，使得内部服务器可以正常提供服务。

- 如果 NAT Server 配置错误，请重新进行正确配置。
- 如果 NAT Server 配置正确，故障仍然存在，请执行步骤 3。

步骤 3 检查外网主机和 NAT Server 外网接口之间的连接及配置

检查 NAT Server 外网接口上的 IP 地址以及为 NAT Server 配置的外网 IP 地址是否正确。例如，是否和其他该网段的地址发生冲突。从外网主机上 ping NAT Server 的外网接口地址，确保外网主机到 NAT Server 之间的连通性。

- 如果外网主机和 NAT Server 外网接口之间的连通性存在问题，请检查并确保连通性正常。
- 如果外网主机和 NAT Server 外网接口之间的连通性正常，故障仍然存在，请执行步骤 4。

步骤 4 检查内网 NAT Server 的网关或路由配置

检查内网服务器上是否配置了正确的路由或者网关，使得发向外网的报文可以正确的送到 NAT 网关。

- 如果 NAT Server 的网关或路由配置有问题，请重新进行正确配置。
- 如果 NAT Server 的网关或路由配置正常，故障仍然存在，请执行步骤 5。

步骤 5 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

版权所有 © 华为技术有限公司

相关告警与日志

相关告警

无

相关日志

无

10.7.3 两次 NAT 故障现象：内网重叠主机无法访问外网服务器

常见原因

本类故障的常见原因包括：

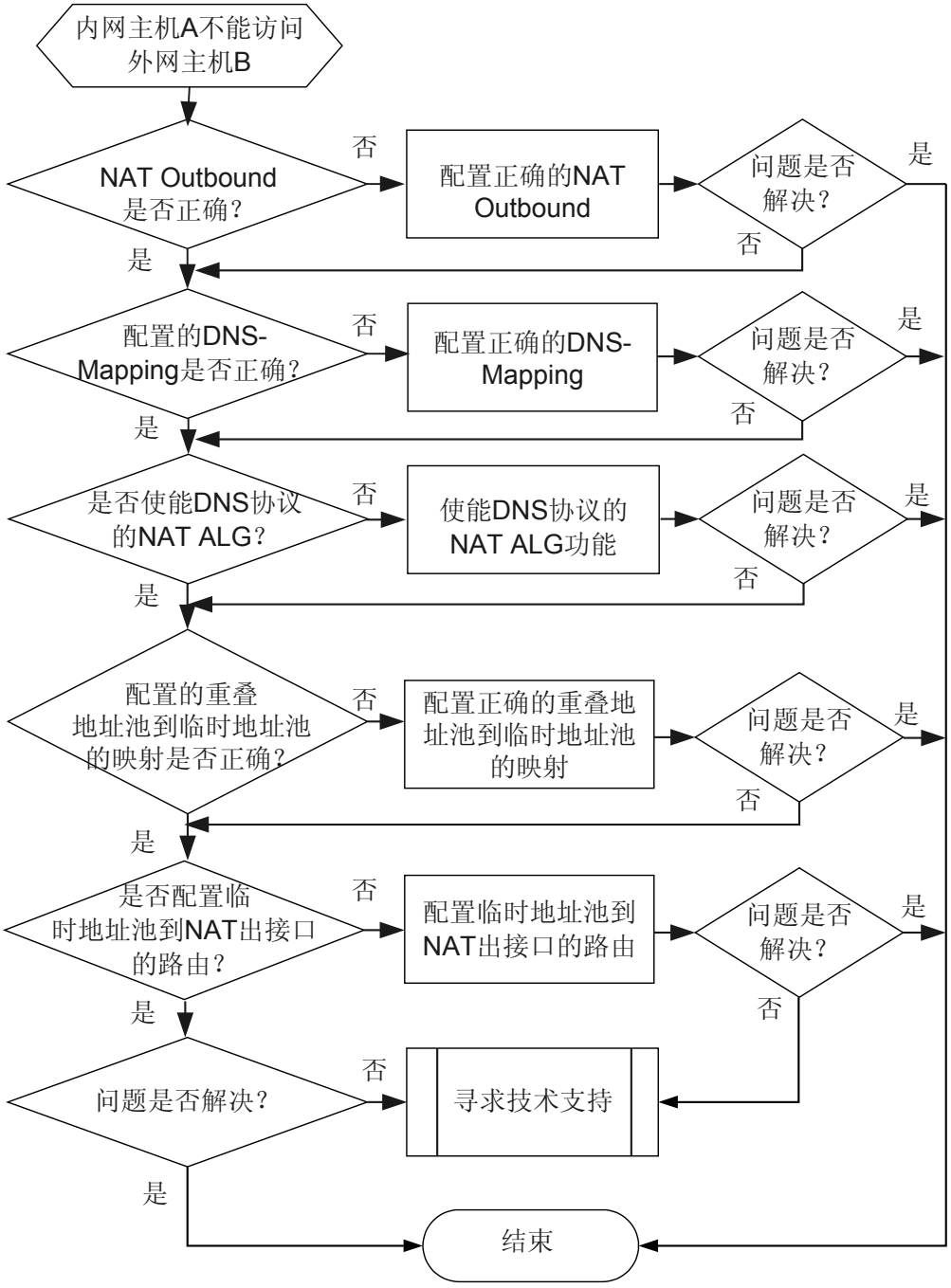
- 用户访问公网的出、入接口状态 Down
- 内网访问公网对应的出接口上配置 NAT Outbound 错误
- 未使能 DNS 协议的 NAT ALG
- 配置的 DNS Mapping 错误（比如，对应的公网地址和外网服务器 IP 地址不同）
- 没有配置从内网临时地址到 NAT 公网出接口的路由

故障诊断流程

详细处理流程，如图 **10-18** 所示。

版权所有 © 华为技术有限公司

图 10-18 两次 NAT 故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

步骤 1 检查配置的 NAT Outbound 是否正确

在 AR2200-S 上执行命令 **display nat outbound**，查看 NAT 出接口上是否配置了 NAT Outbound。

```
[AR2200-S]display  nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------------------------------
 Interface                        Acl      Address-group/IP       Type
 ----------------------------------------------------------------------------------------------------
 GigabitEthernet0/0/1            3180                      1       pat
 ----------------------------------------------------------------------------------------------------
  Total : 1
```

由上可知 NAT Outbound 关联的 ACL 号为 3180，地址池索引为 1。查看 NAT Outbound 引用的地址池是否正确，地址池的配置需要注意：避免外网目的地址和地址池中的地址重复。通过执行命令 **display nat address-group** 查看地址池配置信息。

```
[AR2200-S]display nat address-group 1
NAT Address-Group Information:
--------------------------------------
Index   Start-address      End-address
--------------------------------------
1       202.10.10.10      202.10.10.100
--------------------------------------
Total : 1
```

最后再查看 NAT Outbound 关联的 ACL 规则是否正确，ACL 规则常见问题有：没有配置合适的地址、协议、端口等，导致内网报文无法送出或外网报文无法进入。

执行命令 **display acl 3180** 查看当前 NAT Outbound 关联的 ACL 配置。

```
[AR2200-S]display acl 3180
Advanced ACL 3180, 1 rule
Acl's step is 5
rule 5 permit tcp source 1.1.1.1 0
```

说明

ACL 规则一般配置比较严格，只根据具体的组网需求开放特定的地址段、协议或端口。当某种协议的报文无法通过 NAT 网关时，先检查 ACL 中是否配置了允许该类报文通过的规则。

- 如果 NAT Outbond 配置错误，请修改对应配置。
- 如果 NAT Outbond 配置正确，故障仍然存在，请执行步骤 2。

步骤 2 检查 DNS Mapping 配置是否正确

在 AR2200-S 上执行命令 **display nat dns-map**，查看 DNS Map 是否配置在正确的 NAT 出接口上，是否配置了正确的协议、端口和地址信息。

```
[AR2200-S]display nat dns-map
  NAT DNS mapping information:
  Domain-name : test1
  Global IP   : 10.1.1.1
  Global port : 2012
  Protocol    : tcp

  Total : 1
```

- 如果 DNS Mapping 配置错误，请在系统视图下执行命令 **nat dns-map**，配置正确的 DNS Mapping，再尝试访问主机。
- 如果 DNS Mapping 配置正确，故障仍然存在，请执行步骤 3。

步骤 3 检查是否使能了 DNS 协议的 NAT ALG 功能

在 AR2200-S 上执行命令 **display nat alg**，查看 DNS 的 NAT ALG 是否使能。

版权所有 © 华为技术有限公司

```
[AR2200-S]display nat alg
NAT Application Level Gateway Information:
----------------------------------
  Application           Status
----------------------------------
  dns                   Disabled
  ftp                   Disabled
  rtsp                  Enabled
  sip                   Disabled
----------------------------------
```

- 如果 DNS 的 NAT ALG 未使能，请使用 **nat alg enable** 使能 NAT ALG。
- 如果 DNS 的 NAT ALG 已使能，故障仍然存在，请执行步骤 4。

步骤 4 检查配置的重叠地址池到临时地址池的映射是否正确

在 AR2200-S 上执行命令 **display nat overlap-address**，查看所有已配置的重叠地址池到临时地址池的映射。

```
[AR2200-S]display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:

-------------------------------------------------------------------------------------------------------------
 Id  Overlap-Address  Temp-Address    Pool-Length       Inside-VPN-Instance-Name

-------------------------------------------------------------------------------------------------------------
 1   1.1.1.1          20.20.20.20     34
-------------------------------------------------------------------------------------------------------------
  Total : 1
```

说明

临时地址池是设备上空闲可用的 IP 地址，不能和接口地址、VRRP 地址、NAT 类型地址存在冲突。 Inside-VPN-Instance-Name 表示和主机连接的内网接口所在的 VPN 实例名。

- 如果映射关系不正确，请重新进行正确配置。
- 如果映射关系正确，故障仍然存在，请执行步骤 5。

步骤 5 检查是否配置临时地址池到 NAT 出接口的路由

在 AR2200-S 上执行命令 **display ip routing-table**，查看公网上的所有路由。

```
[AR2200-S]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 99       Routes : 99

Destination/Mask    Proto  Pre  Cost       Flags NextHop         Interface

    10.0.0.0/8     Static   60   0            D   10.164.50.1     Ethernet0/0/0
    10.10.10.10/32 Unr    64   0            D   127.0.0.1       InLoopBack0
```

说明

若主机连接的内网接口所在的 VPN 实例名不为空，则查询路由使用 **display ip routing-table vpn-instance** *vpn-name*。

- 如果没有正确的路由表项，请检查并重新配置路由。
- 如果路由表项正确，故障仍然存在，请执行步骤 5。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。

版权所有 © 华为技术有限公司

- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.8 PKI 故障处理

10.8.1 获取 CA 证书失败的定位思路

常见原因

本类故障的常见原因主要包括：

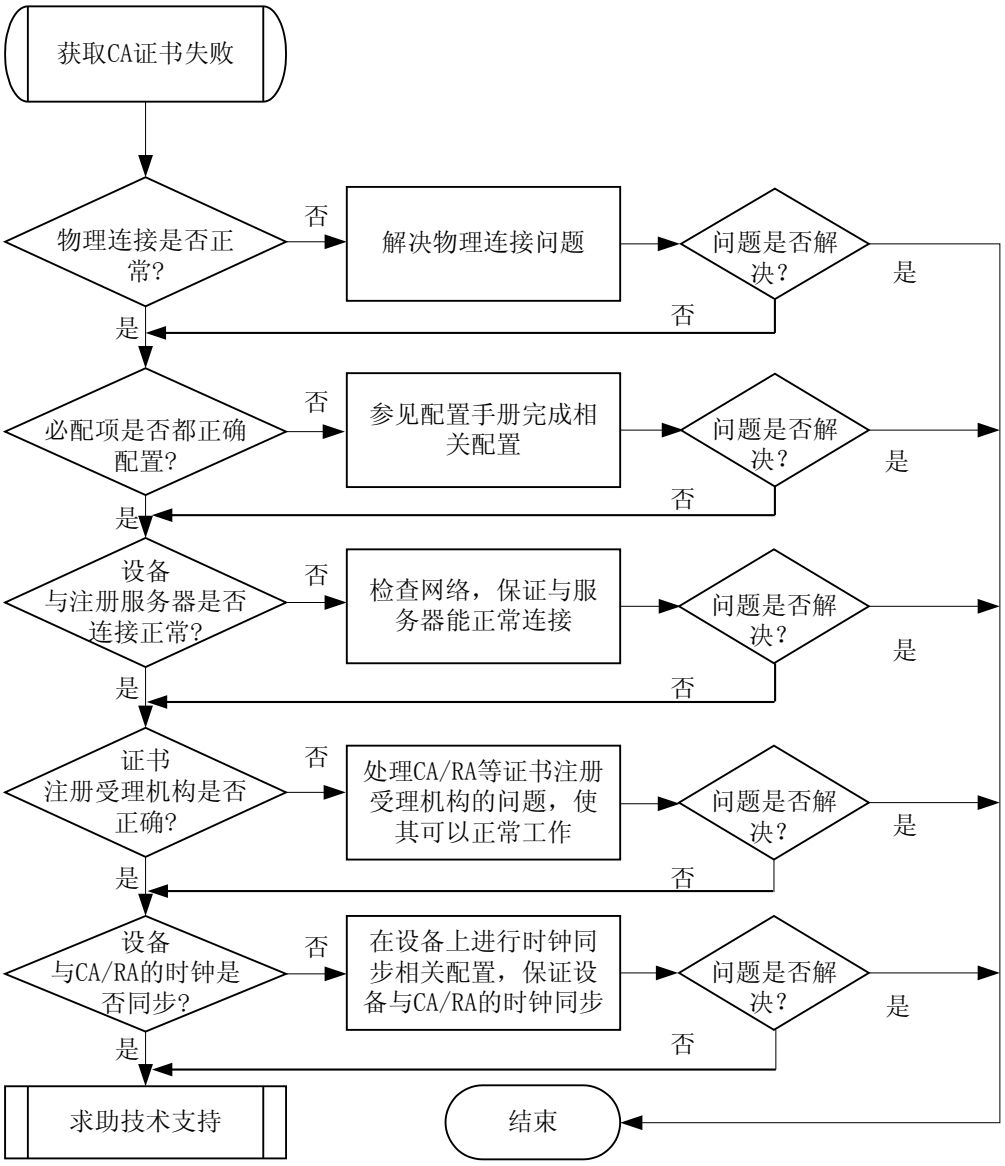
- 网络连接故障，如网线折断，接口松动
- 没有设置信任的 CA 名称
- 证书申请的注册服务器 URL 不正确或未配置
- 证书申请的注册模式不正确(分为 CA 模式和 RA 模式)
- 没有配置证书申请注册受理机构
- CA 证书的指纹配置错误
- 设备的系统时钟与 CA 的时钟不同步

故障诊断流程

获取 CA 证书失败的故障详细处理流程如**图 10-19** 所示。

版权所有 © 华为技术有限公司

图 10-19 获取 CA 证书失败故障处理流程图



故障处理步骤

操作步骤

步骤 1 排除物理连接故障。

步骤 2 检查各必配项是否都正确配置。

执行命令 display pki realm，查看域的必选配置是否正确。

如果配置的 CA ID 不正确，则获取 CA 证书可能失败。

如果配置的注册证书的 URL 不正确，那么获取 CA 证书也可能失败。

版权所有 © 华为技术有限公司

如果用户在域下配置了指纹，那么指纹配置时填写错误将导致无法获取 CA 证书；如果用户在域下没有配置指纹，那么通过命令行获取 CA 证书时需要用户自己输入正确的指纹。

还要查看域的 Enrollment Mode 是否配置正确，如果是 RA 服务器，则 Enrollment Mode 为 RA；如果是 CA 服务器，则 Enrollment Mode 为 CA。 如果配置正确，而故障仍然存在，请执行步骤 3。

步骤 3 通过 ping 命令检查设备与注册服务器是否连接正常。

如果设备和注册服务器连接正常，而故障仍然存在，请执行步骤 4。

步骤 4 检查证书注册受理机构是否正确。

确认证书申请注册受理机构（如 RA、CA 等）配置，如果不正常，请正确配置。

如果正常，而故障仍然存在，请执行步骤 5。

步骤 5 检查设备与 CA/RA 的时钟是否同步。

如果不同步，请配置同步。

如果以上步骤的分析，仍然解决不了问题，请执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.8.2 申请本地证书失败的定位思路

常见原因

本类故障的常见原因主要包括：

- 网络连接故障，如网线折断，接口松动
- 没有设置信任的 CA 名称
- 证书申请的注册模式不正确(分为 CA 模式和 RA 模式)
- CA 证书的指纹配置错误
- 证书申请的注册服务器 URL 不正确或未配置

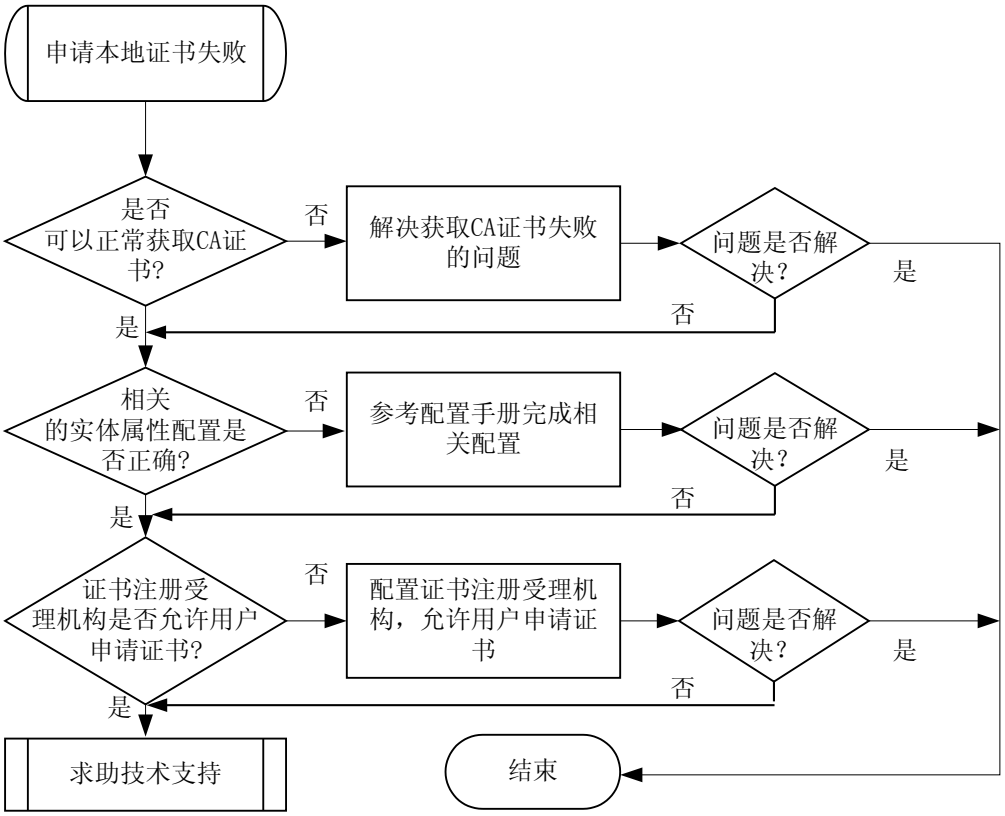
版权所有 © 华为技术有限公司

- 没有配置证书申请注册受理机构
- 设备的系统时钟与 CA 的时钟不同步
- 没有配置实体中必配参数

故障诊断流程

申请本地证书失败的故障详细处理流程如图 10-20 所示。

图 10-20 申请本地证书失败故障处理流程图



故障处理步骤

操作步骤

步骤 1 检查是否可以正常获取 CA 证书。

如果无法正常获取 CA 证书，检查获取 CA 证书失败的原因。

如果 CA 证书可以正常获取，执行步骤 2。

步骤 2 检查相关的实体属性配置是否正确。

查看实体的必配选项是否进行了配置，以及域下配置的实体名是否和实体的名称一致。

如果配置正确，而故障仍然存在，请执行步骤 3。

版权所有 © 华为技术有限公司

步骤 3 检查证书注册受理机构。

确认证书注册受理机构（如 RA、CA 等）配置，是否允许用户申请证书。

如果以上步骤的分析，仍然解决不了问题，请执行步骤 4。

步骤 4 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

10.8.3 CRL 获取失败的定位思路

常见原因

本类故障的常见原因主要包括：

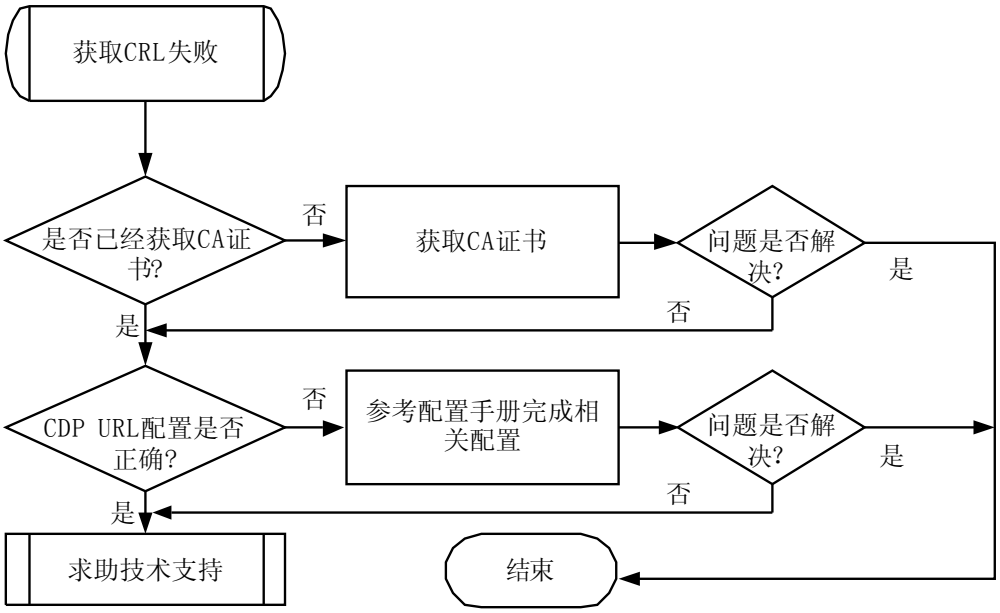
- 获取 CRL 之前未先取得 CA 证书
- 未正确设置 CRL 发布点 URL

故障诊断流程

获取 CRL 失败的故障详细处理流程如图 10-21 所示。

版权所有 © 华为技术有限公司

图 10-21 获取 CRL 失败的故障处理流程图



故障处理步骤

操作步骤

步骤 1 检查是否已经获取 CA 证书。

通过 **display pki certificate** 命令查看 CA 证书是否存在。

如果 CA 证书未获得，请先获取 CA 证书。

如果 CA 证书已经获取，而故障仍然存在，请执行步骤 2。

步骤 2 检查 CDP URL 配置是否正确。

如果已经配置 CDP URL，检查该配置是否正确。

如果以上步骤的分析，仍然解决不了问题，请执行步骤 3。

步骤 3 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

版权所有 © 华为技术有限公司

相关日志

无

版权所有 © 华为技术有限公司

11 可靠性类

关于本章

11.1 接口备份故障处理
11.2 BFD 故障处理
11.3 VRRP 故障处理

版权所有 © 华为技术有限公司

11.1 接口备份故障处理

11.1.1 接口备份失效的定位思路

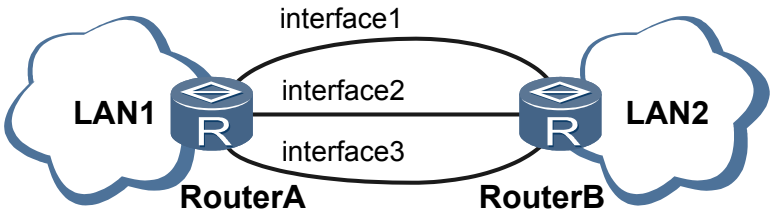
常见原因

如图 11-1 所示，RouterA 和 RouterB 连接。

RouterA 上的多个接口形成备份关系：

- 接口 interface1 作为主接口。
- 接口 interface2 和 interface3 作为接口 interface1 的备份接口。

图 11-1 接口备份的组网图



接口备份失效包括以下几种情况：

- 备份接口在主接口发生故障后不能启用生效
- 负载分担情况下，备份接口不能与主接口形成负载分担，即主备接口不能同时 UP
- 负载分担情况下，流量没有分担到多个接口上

本类故障的常见原因主要包括：

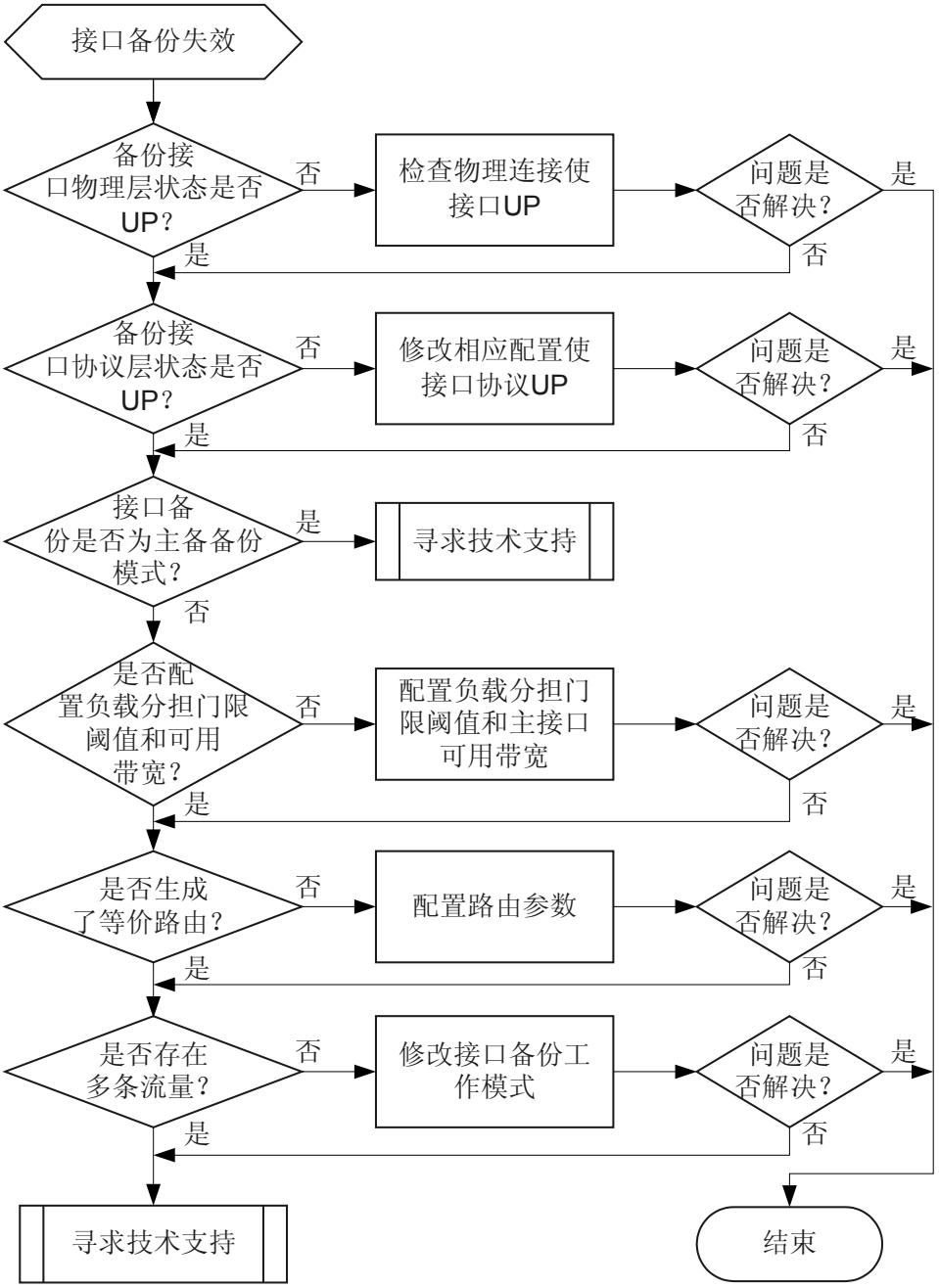
- 备份接口物理层没有 UP
- 备份接口协议层没有 UP
- 负载分担方式下：
  - 没有配置负载分担门限阈值和主接口可用带宽
  - 没有生成等价路由
  - 不存在多条流量

故障诊断流程

详细处理流程如图 11-2 所示。

版权所有 © 华为技术有限公司

图 11-2 接口备份失效故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查备份接口物理层状态是否 UP。

在本端设备和对端设备上分别执行 **display interface** *interface-type interface-number* 命令，查看 **current state** 字段。

版权所有 © 华为技术有限公司

- 如果接口状态为 **DOWN**，请检查接口连线以及接口的相关参数配置是否正确。
- 如果接口状态为 **UP**，请执行步骤 2。

步骤 2 检查备份接口协议层状态是否 UP。

在本端设备和对端设备上分别执行 **display interface** *interface-type interface-number* 命令，查看 **Line protocol current state** 字段。

- 如果接口协议层状态为 **DOWN**，请检查接口 IP 地址以及相关协议参数配置是否正确。

  说明

  当 Dialer 接口做备份接口时，必须配置 IP 地址用于触发拨号，并在接口上配置路由协议。

  当主接口发生故障，Dialer 接口作为备份接口被启用时，路由协议会通过 Dialer 接口发送协议报文，从而触发 Dialer 接口拨号，并生成路由。

- 如果接口协议层状态为 **UP**，请执行步骤 3。

步骤 3 检查接口备份的工作模式是否为主备备份。

在主接口的接口视图下执行 **display this** 命令，查看主接口上是否配置了负载分担阈值和主接口带宽。

- 如果没有相应参数的设置，说明接口备份工作方式为主备备份。请根据实际组网需求判断接口备份的方式是否为主备备份。
  - 如果实际组网需求为主备备份方式，请执行步骤 6。
  - 如果实际组网需求为负载分担方式，请执行 **standby threshold** *enable-threshold disable-threshold* 命令，配置负载分担模式下负载门限的上限和下限阈值；执行 **standby bandwidth** *size* 命令，配置主接口的可用带宽。
- 如果已经配置相应参数，说明接口备份工作方式为负载分担，请执行步骤 4。

步骤 4 检查是否生成等价路由。

对同一目的地址，接口备份如果要形成负载分担，使流量从多个接口发送，必须要生成等价路由。执行 **display ip routing-table** 命令，查看是否生成等价路由。如下所示，表明已经形成等价路由。

```
<Huawei>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        2.2.2.0/24  Static  60    0           RD  192.168.1.2     GigabitEthernet1/0/0
                    Static  60    0           RD  192.168.2.2     GigabitEthernet2/0/0
```

- 如果没有生成等价路由，请检查并修改相关路由设置。

  常用方法如下：

  - 修改相应路由参数，如路由开销等参数；
  - 直接配置静态路由，如上显示。

  说明

  这里是针对同一目的地址的流量的前提下进行描述。如果网络中存在多条不同目的地址的流量，并且都从主接口和备份接口发送，即使没有等价路由，也可形成负载分担。

  形成负载分担的原则如下:

  - 当主备有多个接口同时工作时，这些接口上必须都有路由
  - 如果要维持负载分担的稳定状态，还必须保证主接口的流量负载大于下限阈值，否则会关闭备份接口

版权所有 © 华为技术有限公司

- 如果已经生成等价路由，请执行步骤 5。

步骤 5 请检查链路上是否存在多条流量。

在生成等价路由之后，设备转发报文时，会根据一定的 HASH 算法选择一条路由发送报文。如果只有一条流量，则不能分担到多条链路上发送。只有存在多条流量时，设备才能把流量分到多条链路。请根据实际网络情况进行判断。

- 如果仅存在一条流量从主接口发送，请将设备的接口备份工作模式改成主备备份。
- 如果已经存在多条流量，故障依然存在，请执行步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

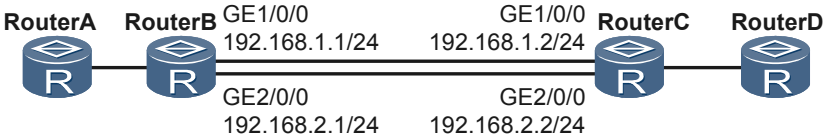
11.1.2 故障案例

负载分担模式下备份接口反复 Up/Down

网络环境

在如图 11-3 的组网下，RouterB 上配置接口备份，工作模式为负载分担。当 RouterA 向 RouterD 发送流量时，备份接口反复 Up/Down。

图 11-3 负载分担模式下备份接口反复 Up/Down 组网图



故障分析

1. 查看 RouterB 上主接口和备份接口的物理连线情况以及接口配置，发现两个接口连线和接口的相应配置均正确。在不配置接口备份的情况下，两个接口单独均可以正常工作。
2. 查看 RouterB 上接口备份的配置。在 RouterB 主接口下，执行 **display this** 命令，发现配置如下所示，说明已经配置了负载分担门限阈值和主接口可用带宽，说明接口备份的工作方式为负载分担。

版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet1/0/0
ip address 192.168.1.1 255.255.255.0
standby interface GigabitEthernet 2/0/0 30
bandwidth 10000
standby threshold 80 20
#
```

3. 在 RouterB 上执行 **display ip routing-table** 命令，发现已经生成等价路由。

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        2.2.2.0/24  Static  60    0           RD  192.168.1.2     GigabitEthernet1/0/0
                    Static  60    0           RD  192.168.2.2     GigabitEthernet2/0/0
```

4. 通过分析组网，发现只有 RouterA 有发送给 RouterD 的流量从 RouterB 的主备接口发送。在没有流量的情况下，主接口 GE1/0/0 状态为 UP，备份接口 GE2/0/0 状态为 STANDBY。当发送流量并超过负载分担门限阈值时，接口备份模块启用备份接口 GE2/0/0。由于只存在一条数据流，并且此时按照 Hash 算法选中备用接口，则所有的报文都会从备用接口发送。此时，主接口 GE1/0/0 的负载立刻变为 0。当接口备份检测到只有主接口的负载降低下限阈值以下时，则会关闭备份接口。因此出现备份接口反复 Up/Down 的现象。

操作步骤

步骤 1 在 RouterB 上的主接口的接口视图下，执行 **undo standby bandwidth** 命令用来恢复缺省配置。

步骤 2 执行 **undo standby threshold** 命令取消负载分担门限。

完成上述操作后，故障排除。

----结束

案例总结

建议在如下情况下使用接口备份流量负载分担模式:

- 单独使用主接口时，主接口的流量大于上限阈值
- 流量负载分担后，在主接口上的流量仍然大于下限阈值，保证不会关闭备份接口
- 启用备份接口后，通往多个目的地址的流量能够分担到主备接口上，或者通往同一目的地址的流量在主备接口上存在等价路由：
  - 主备接口存在不同的路由

```
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
2.2.2.0/24  Static  60      0    RD        192.168.1.2     GigabitEthernet1/0/0
3.3.3.0/24  Static  60      0    RD        192.168.2.2     GigabitEthernet2/0/0
```

  - 主备接口存在等价路由

```
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
2.2.2.0/24  Static  60      0    RD        192.168.1.2     GigabitEthernet1/0/0
            Static  60      0    RD        192.168.2.2     GigabitEthernet2/0/0
```

11.2 BFD 故障处理

版权所有 © 华为技术有限公司

11.2.1 BFD 会话无法 Up 的定位思路

常见原因

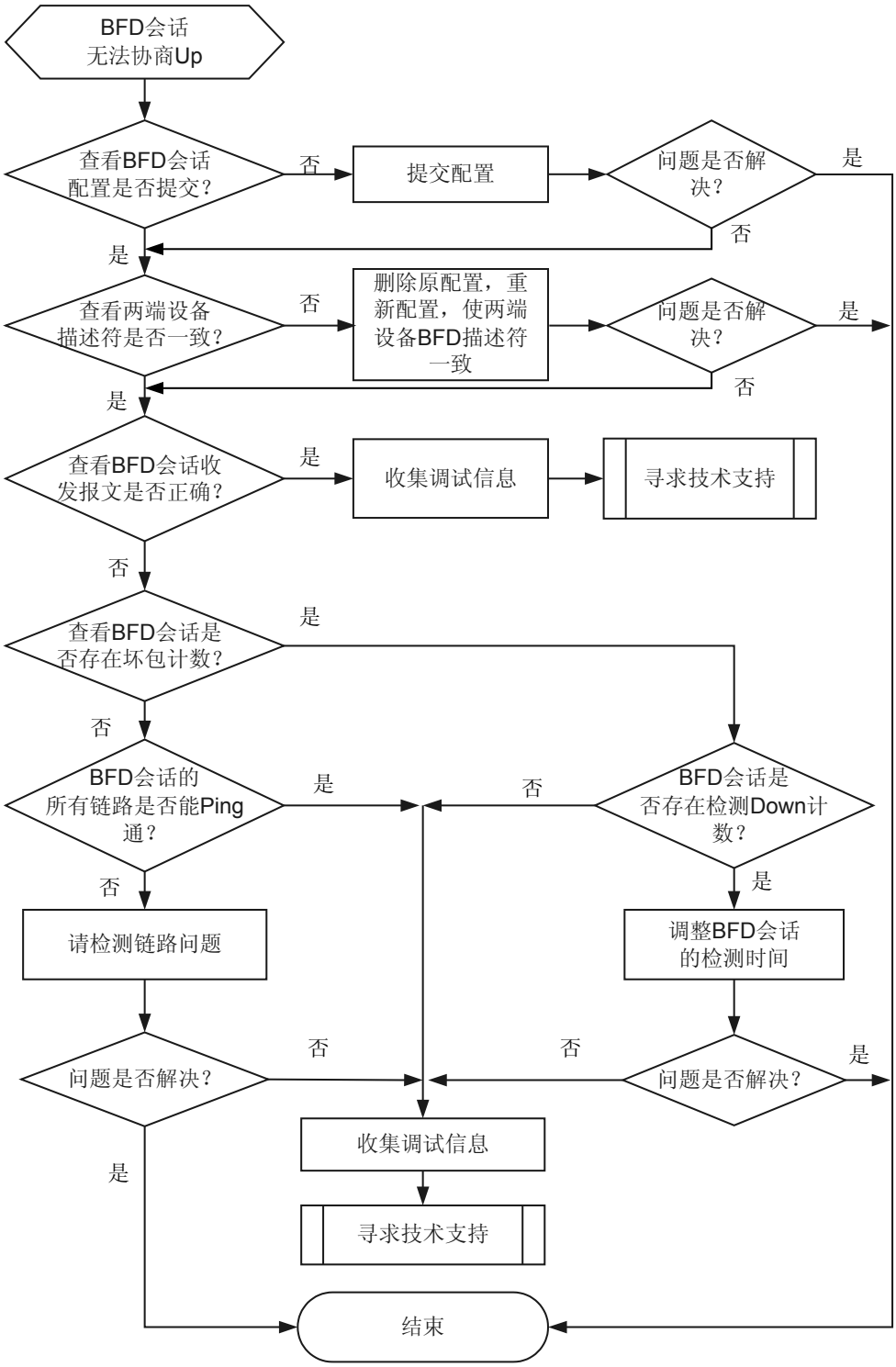
本类故障的常见原因主要包括：

- 设备两端配置的描述符不一致。
- BFD 会话检测的链路存在故障，导致 BFD 报文无法进行交互。
- BFD 会话频繁震荡。

版权所有 © 华为技术有限公司

故障诊断流程

图 11-4 BFD 会话无法 Up 故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 执行 **display current-configuration** 命令检查 BFD 会话的配置是否提交。

- 如果查看到 **commit** 字段，表示 BFD 会话已经提交，请执行**步骤 2**。
- 如果没有查看到 **commit** 字段，则表示 BFD 会话未提交。用户需要在 BFD 会话视图下执行 **commit** 命令，然后使用 **display bfd session all** 命令查看 BFD 会话是否 Up。
  - 如果“State”字段的值为 Up，则表明 BFD 会话已经建立。
  - 如果“State”字段的值为非 Up，请执行**步骤 2**。

步骤 2 执行 **display current-configuration** 命令，查看两端设备配置的描述符是否一致。

- 如果不一致，请先执行 **undo bfd** 命令删除原有 BFD 会话，再执行 **bfd bind peer-ip** 命令重新建立 bfd 会话，最后执行 **discriminator** { **local** *discr-value* | **remote** *discr-value* }命令配置设备本地和远端描述符，使两端设备保持一致。请执行**步骤 3**。
- 如果一致，请执行**步骤 4**。

步骤 3 执行 **display bfd session all** 命令查看 BFD 会话是否 Up。

- 如果“State”字段的值为 Up，则表明 BFD 会话已经建立。
- 如果“State”字段的值为非 Up，请执行**步骤 4**。

步骤 4 重复执行 **display bfd statistics session all** 命令，查看 BFD 会话收发报文的统计信息。

- 如果 **Received Packets** 字段的计数没有增加，请执行**步骤 5**。
- 如果 **Send Packets** 字段的计数没有增加，请执行**步骤 6**。
- 如果 **Received Packets** 字段和 **Send Packets** 字段的计数都正常增加，请执行**步骤 9**。
- 如果 **Received Packets** 字段、**Send Packets** 字段、**Received Bad Packets** 字段和 **Send Bad Packets** 字段计数都没有增加，请执行**步骤 7**。
- 如果 BFD 统计数中 **Down Count** 字段的计数增加，说明 BFD 会话在震荡，请执行**步骤 7**。

步骤 5 重复执行 **display bfd statistics session all** 命令，查看 **Received Bad Packets** 字段计数是否有增加。

- 如果 **Received Bad Packets** 字段的计数增加，说明 BFD 会话从对端收到了报文，但此报文被丢弃，请执行**步骤 9**。
- 如果 **Received Bad Packets** 字段的计数没有增加，说明本端没有收到 BFD 报文，请执行**步骤 7**。

步骤 6 重复执行 **display bfd statistics session all** 命令查看 **Send Bad Packets** 字段计数是否有增加。

- 如果 **Send Bad Packets** 字段的计数增加，说明 BFD 会话发送的报文被丢弃，请执行**步骤 9**。

版权所有 © 华为技术有限公司

- 如果 **Send Bad Packets** 字段的计数没有增加，说明本端没有将 BFD 报文发送到对端，请执行**步骤 7**。

步骤 7 重复执行 **display bfd statistics session all** 命令，如果 BFD 会话没有 Up，请执行 **Ping** 命令检查 BFD 会话之间的链路转发是否正常。

- 如果 ping 不通，请参见 **Ping 不通问题**排除转发故障。
- 如果能 ping 通，请执行**步骤 8**。

步骤 8 使用 **display current-configuration** 命令，查看 BFD 会话的 **min-tx-interval** 和 **min-rx-interval** 信息，检查 BFD 会话的检测时间是否大于链路的延迟时间。

- 如果 BFD 会话的检测时间小于链路的延迟时间，则请执行 **detect-multiplier** 命令、**min-rx-interval** 和 **min-tx-interval** 命令调整 BFD 会话的检测时间，使之大于链路的延迟时间。
- 如果 BFD 会话的检测时间大于链路的延迟时间，请执行**步骤 9**。

步骤 9 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

11.2.2 BFD 会话检测 Down 影响接口转发的定位思路

常见原因

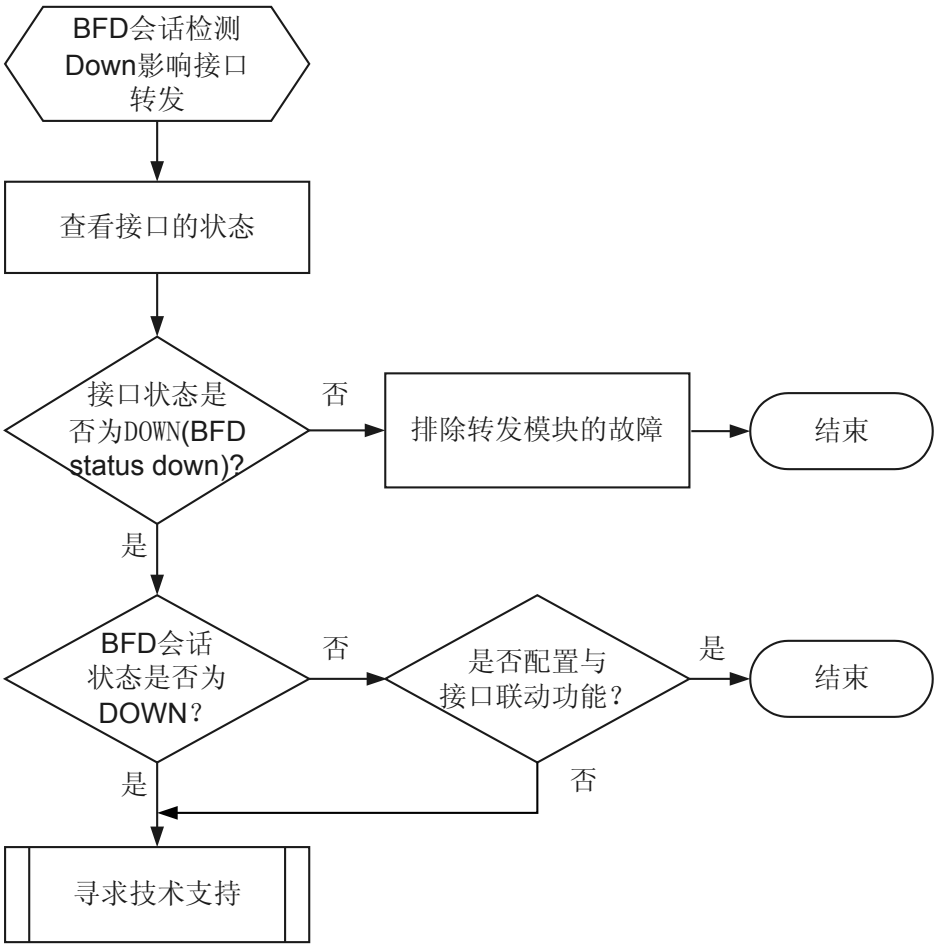
本类故障的常见原因主要包括：

- 配置了 BFD 会话与接口联动功能。

版权所有 © 华为技术有限公司

故障诊断流程

图 11-5 BFD 会话检测 Down 影响接口转发故障诊断流程图



故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 执行 **display interface** *interface-type interface-number* 命令查看 BFD 会话绑定的接口的状态。

- 如果“Line protocol current state”字段的值为 **DOWN(BFD status down)**，表明当前接口的状态受 BFD 会话的影响，BFD 会话检测到链路故障后，会将此接口的状态置为 **BFD status down**，请执行**步骤 2**。
- 如果 Line protocol current state 字段的值为 **UP**，但是接口不可转发，则请参见 **Ping 不通问题**，排除转发模块的故障。

版权所有 © 华为技术有限公司

步骤 2 执行 **display bfd session all** 命令，查看 BFD 会话的状态。

- 如果 BFD 会话的状态为 **Down**，请执行步骤 3。
- 如果 BFD 会话的状态为 **Up**，请执行步骤 4。

步骤 3 执行 **display current-configuration configuration bfd-session** 查看 BFD 会话的配置信息，检查是否配置了 **process-interface-status** 命令。

- 如果配置了 **process-interface-status** 命令，表明此接口的状态是因为 BFD 会话检测 Down，接口被置为 DOWN(BFD status down)状态，导致接口不可转发。
- 如果没有配置 **process-interface-status** 命令，请执行步骤 4。

步骤 4 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

11.2.3 修改 BFD 会话检测参数不生效的定位思路

常见原因

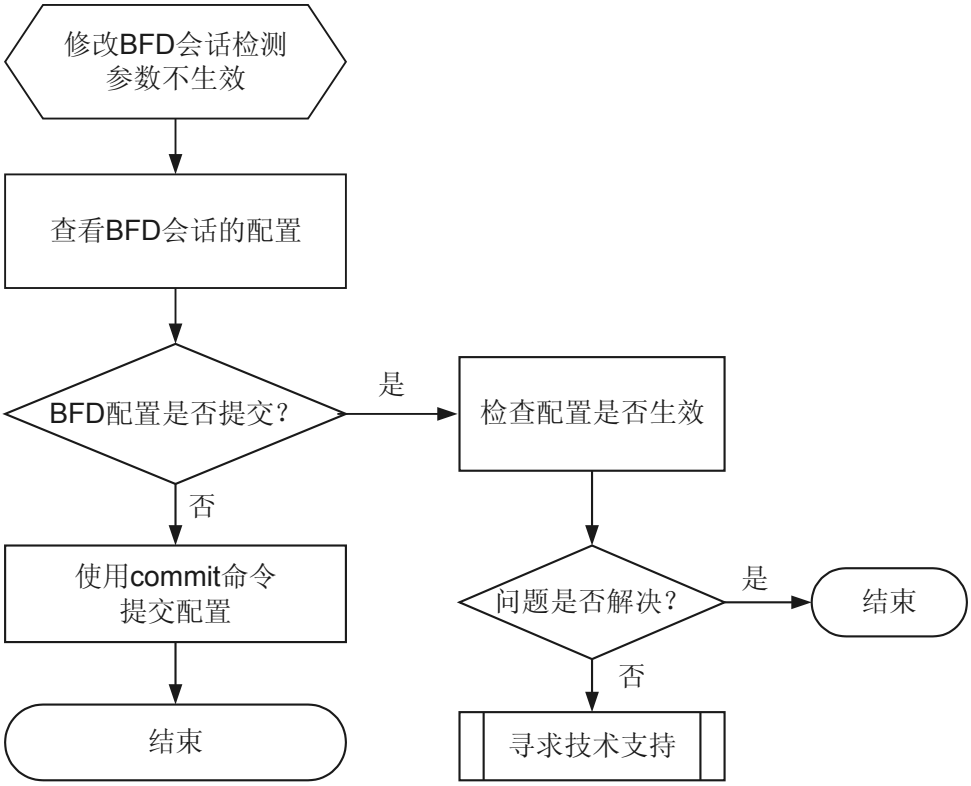
本类故障的常见原因主要包括：

- 修改 BFD 会话后，没有提交会话的配置信息。

版权所有 © 华为技术有限公司

故障诊断流程

图 11-6 修改 BFD 会话检测参数不生效故障诊断流程图



故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 执行 **display current-configuration configuration bfd-session** 查看 BFD 会话的配置信息，检查是否配置了 **commit** 命令。

- 如果配置了 **commit** 命令，表明修改 BFD 会话的检测参数后已经提交，请执行**步骤 3**。
- 如果没有配置 **commit** 命令，表明修改 BFD 会话的检测参数后未提交，用户需要执行 **commit** 命令提交配置,请执行**步骤 2**。

步骤 2 执行 **display bfd session all** 命令，查看 BFD 检测相关参数是否为配置的值。

- 如果是，表明参数修改已经生效。
- 如果不是，请执行**步骤 3**。

版权所有 © 华为技术有限公司

步骤 3 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

11.2.4 动态 BFD 会话没有创建成功的定位思路

常见原因

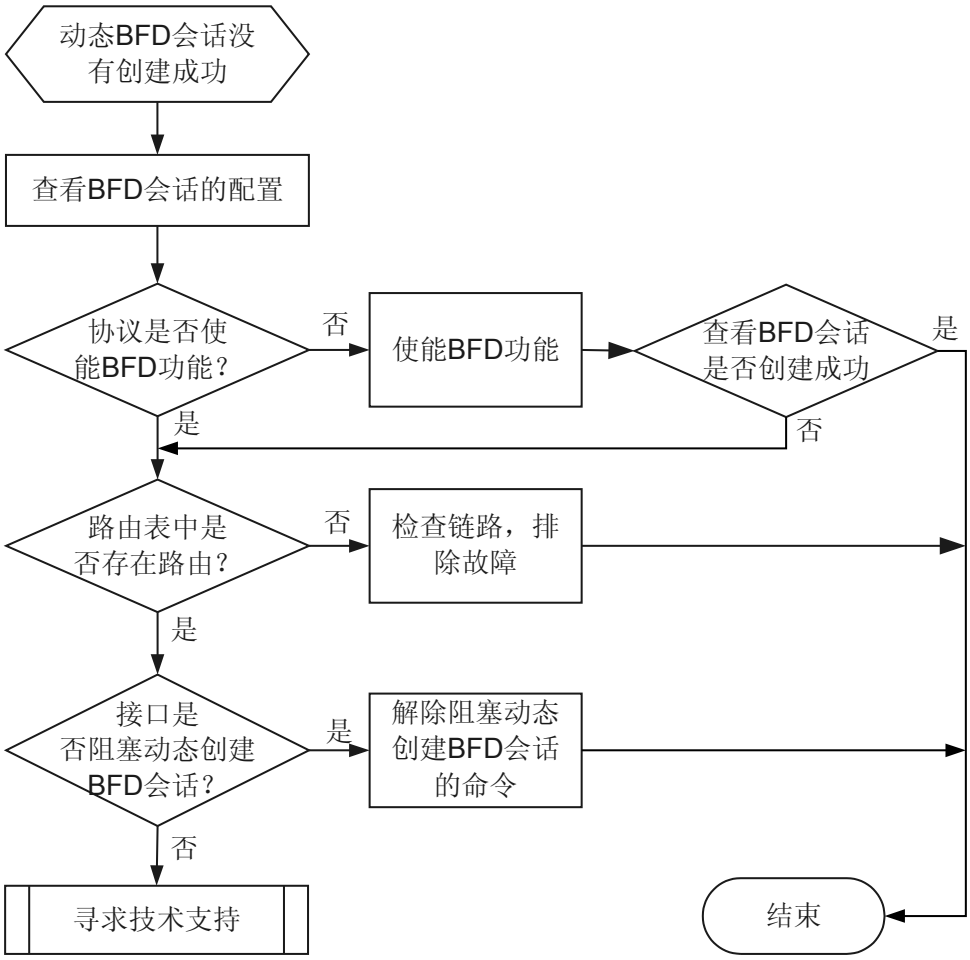
本类故障的常见原因主要包括：

- 相关协议中没有使能 BFD 功能。
- 路由表中没有 BFD 会话创建 Peer 的路由。
- 接口阻止动态创建 BFD 会话。

版权所有 © 华为技术有限公司

故障诊断流程

图 11-7 动态 BFD 会话没有创建成功故障诊断流程图



故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 执行 **display current-configuration configuration bfd** 命令查看协议是否使能了 BFD 功能。

- 如果没有使能 BFD 功能，则请在协议下使能 BFD 功能，并执行**步骤 2**。
- 如果已经使能了 BFD 功能，请执行**步骤 3**。

步骤 2 执行 **display bfd session all** 命令，查看“State”字段的值。

版权所有 © 华为技术有限公司

- 如果“State”值为 Up，则表示 BFD 动态会话创建成功。
- 如果“State”值不为 Up，请执行**步骤 3**。

步骤 3 执行 **display ip routing-table** 命令，查看是否有 BFD 会话检测链路的路由。

- 如果有路由，请执行**步骤 4**。
- 如果没有路由，表明协议下发创建 BFD 会话失败，请参见 **Ping 不通问题**，检查链路问题。

步骤 4 先执行 **interface** *interface-type interface-number* 命令进入接口视图，再执行 **display this** 命令查看接口下的配置信息，检查是否存在阻止接口动态创建 BFD 会话的命令行。

- 如果有，则执行 **undo ospf bfd block** 命令解除阻止接口动态创建。并执行 **display bfd session all** 命令，查看会话是否成功创建，如果不成功请执行**步骤 5**。
- 如果没有，请执行**步骤 5**。

步骤 5 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

11.3 VRRP 故障处理

11.3.1 故障案例

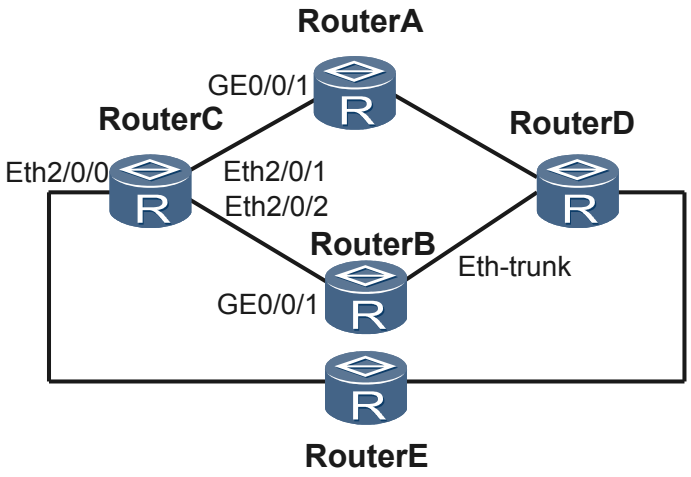
VRRP 环境中数据包丢失

网络环境

在如**图 11-8** 所示的网络中，部署了 VRRP 业务，RouterA 和 RouterB 分别作为 VRRP 备份组的 Master 和 Backup 设备，RouterC 作为交换机连接 RouterA 和 RouterB。

版权所有 © 华为技术有限公司

图 11-8 VRRP 组网图



配置完成后，发现从 RouterE 发往 RouterD 的设备出现了严重丢包。

故障分析

1. 依次在 RouterA 和 RouterB 上执行 **display vrrp** [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics** 命令，检查 VRRP 备份组 RouterA 的 GE0/0/1 和 RouterB 的接口 GE0/0/1 的流量状态。发现 Master 设备 RouterA 的 GE0/0/1 接口有少量流量，Backup 设备 RouterB 的 GE0/0/1 接口没有流量。

   在 RouterC 上执行 **display interface counters** 命令，检查 RouterC 接口 Eth2/0/0、Eth2/0/1、Eth2/0/2 的流量状态，发现 Eth2/0/1 和 Eth2/0/2 的流量状态和 RouterA 的 GE0/0/1、RouterB 的 GE0/0/1 流量状态一致，但 RouterC 的 Eth2/0/0 有大量流量。说明流量在 RouterC 发生丢失。

2. 在 RouterC 上执行 **display mac-address dynamic** 命令，检查 MAC 表项，发现学到的 RouterA 的 MAC 地址是从 Eth2/0/0 发出去的，而连接主、备设备的出接口分别是 Eth2/0/1 和 Eth2/0/2，MAC 地址表项错误。如下：

```
MAC address table of slot 1:
------------------------------------------------------------------------------
MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/
               VSI/SI                                              MAC-Tunnel
------------------------------------------------------------------------------
0000-0a0a-0102 1           -      -      Eth2/0/0        dynamic   -
0000-5e00-0101 1           -      -      Eth2/0/0        dynamic   -
0098-0113-0005 1           -      -      Eth2/0/0        dynamic   -
0018-824f-f5d1 1           -      -      Eth2/0/2        dynamic   -
------------------------------------------------------------------------------
```

3. 在 RouterC 上执行 **display current-configuration interface** *interface-type interface-number* 命令，查看 Eth2/0/0 的配置。如下：

```
#
 interface Ethernet2/0/0
  undo shutdown
  loopback internal
  portswitch
  port default vlan 1
```

   看出 Eth2/0/0 接口配置了环回，即发往 Eth2/0/0 接口的流量会原样返回。

版权所有 © 华为技术有限公司

4. 在 RouterC 上执行 **display interface counters** 命令，查看 Eth2/0/0、Eth2/0/1、Eth2/0/2 接口的流量，发现 Eth2/0/0 有大量流量。判断是由于该端口的配置导致流量丢失。但是 Eth2/0/2 也有少量流量通过。

5. 在 RouterC 上多次执行 **display mac-address dynamic** 命令，检查 MAC 表项，交换机不同时间从接口 Eth2/0/0 和 Eth2/0/1 都学到相同的 MAC 地址 **0000-5e00-0101**。如下：

```
[RouterC] display mac-address dynamic
      MAC address table of slot 1:
      -------------------------------------------------------------------------------
      MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/
                     VSI/SI                                              MAC-Tunnel
      -------------------------------------------------------------------------------
      0000-0a0a-0102 1           -      -      Eth2/0/0         dynamic   -
      0000-5e00-0101 1           -      -      Eth2/0/0         dynamic   -
      0098-0113-0005 1           -      -      Eth2/0/2         dynamic   -

      0018-824f-f5d1 1           -      -      Eth2/0/0         dynamic   -
      -------------------------------------------------------------------------------
      Total matching items on slot 1 displayed = 4
      [RouterC] display mac-address dynamic
      MAC address table of slot 1:
      -------------------------------------------------------------------------------
      MAC Address    VLAN/       PEVLAN CEVLAN Port            Type      LSP/
                     VSI/SI                                              MAC-Tunnel
      -------------------------------------------------------------------------------
      0000-0a0a-0102 1           -      -      Eth2/0/0         dynamic   -
      0000-5e00-0101 1           -      -      Eth2/0/1         dynamic   -
      0098-0113-0005 1           -      -      Eth2/0/2         dynamic   -
      0018-824f-f5d1 1           -      -      Eth2/0/0         dynamic
-
      -------------------------------------------------------------------------------
      Total matching items on slot 1 displayed=4
```

VRRP 的原理是优先级高的作为 Master，Master 设备默认以 1 秒为周期向 Backup 设备发送 VRRP 通告报文。如果 Backup 设备三次收不到 Master 设备发送的 VRRP 通告报文就会升为 Master，并且发送 VRRP 通告报文。正常情况 ackup 设备不发送 VRRP 通告报文。

说明

配置的时候如果有一台路由器的 IP 地址与 Virtual IP Address 一致，则其一直为 Master。

Master 设备发送 VRRP 通告报文后，报文通过交换机到达 Backup 设备。在交换机上进行 MAC 地址学习，将源 MAC 地址 0000-5e00-0101、VLAN ID 和入端口记录在 MAC 地址表中。流量发送过来后，交换机查 MAC 地址表，将流量从与 Master 设备相连的端口转发出去。主、备发生变化时，原来的 Backup 设备会发送 VRRP 通告报文，交换机重新进行 MAC 地址学习，记录新的出端口。

针对该组网，交换机在收到 VRRP 通告报文后，学习到 Master VRRP 端口的 MAC 地址表项，并向所有的 VLAN ID 为 1 的端口发送该报文。Eth2/0/0 属于 VLAN 1，也会收到交换机发送的 VRRP 通告报文。由于 Eth2/0/0 配置了端口环回功能，报文会从 Eth2/0/0 原封不动的返回，这样就会在 MAC 表中记录 Eth2/0/0 和 MAC 地址 0000-5e00-0101 的对应关系，将以前正确的 MAC 表项覆盖掉。

因此，每隔 1 秒，Master 发送 VRRP 通告报文时，交换机就会出现 MAC 地址表项交替覆盖一次。交换机在第一次学习的 MAC 地址表项是正确的，流量可以正常转发。交换机在第二次学习的 MAC 地址表项是错误的。只有在 MAC 地址表项正确的瞬间，流量可以正常转发，其他时间流量不能正常转发。导致流量丢失。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

版权所有 © 华为技术有限公司

步骤 2 执行命令 **interface** *interface-type interface-number*，进入 Eth2/0/0 接口视图。

步骤 3 执行命令 **undo loopback**，删除该接口上环回的配置。

完成上述操作后，流量不再丢失，故障排除。

----结束

案例总结

二层设备的接口环回会导致 MAC 地址表学习异常，应避免二层接口配置环回功能。

版权所有 © 华为技术有限公司

12 VPN 类

关于本章

12.1 GRE 故障处理
针对典型的 GRE 组网环境，介绍配置 GRE 时要注意的事项，故障处理的流程和详细的故障处理步骤。

12.2 IPSec 故障处理

12.3 SSL VPN 故障处理

12.4 DSVPN 故障处理

版权所有 © 华为技术有限公司

12.1 GRE 故障处理

针对典型的 GRE 组网环境，介绍配置 GRE 时要注意的事项，故障处理的流程和详细的故障处理步骤。

12.1.1 无法 Ping 通对端 Tunnel 接口 IP 地址的定位思路

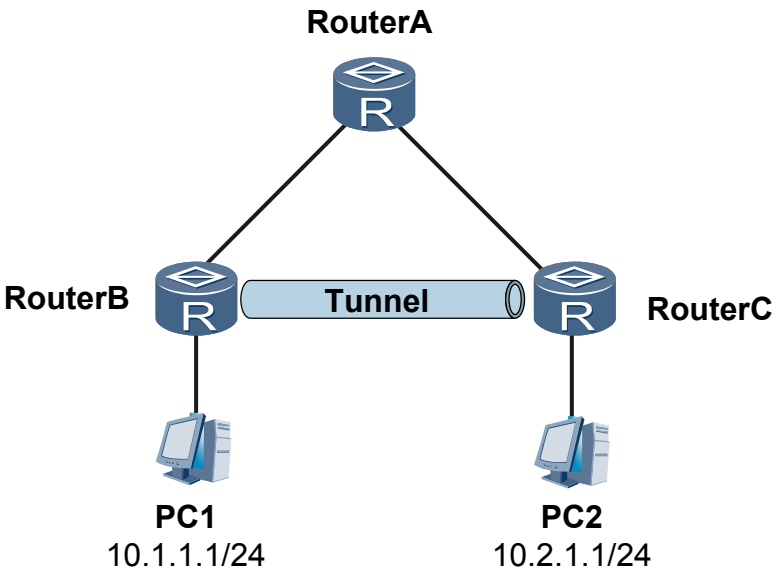
常见原因

- Tunnel 两端封装模式不一致
- 未配置 IP 地址，或者未指定源地址和目的地址
- Tunnel 的源和目的地址之间不存在路由

故障诊断流程

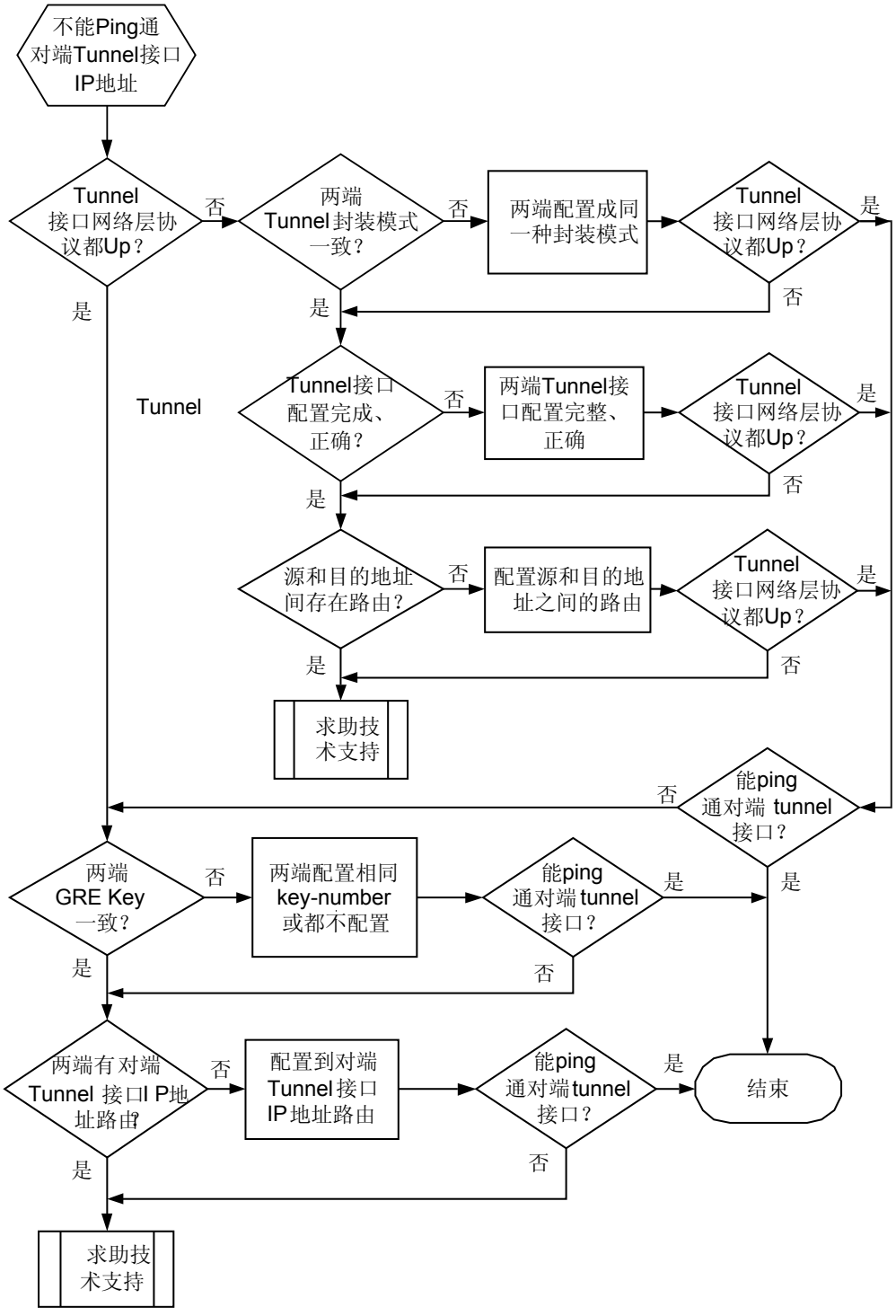
针对图 12-1 所示的网络，在配置各设备后如果发现 PC1 和 PC2 不能互相访问。请使用下面的故障诊断流程，如图 12-2 所示。

图 12-1 GRE 典型组网图



版权所有 © 华为技术有限公司

图 12-2 GRE 故障诊断流程图



故障处理步骤

说明

请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。

版权所有 © 华为技术有限公司

操作步骤

- 一端或两端 Tunnel 接口网络层协议为 Down
  1. 检查两端 tunnel 的封装模式是否一致

     可以在该 tunnel 的接口视图下执行 **display this interface** 命令来检查两端 tunnel 的封装模式是否一致。如果显示为 **Tunnel protocol/transport GRE/IP** 说明封装模式为 GRE。

     - 如果两端的封装模式不相同，请在 tunnel 接口视图下执行 **tunnel-protocol** 命令重新配置隧道封装方式。

       说明

       重新配置 tunnel 的封装协议后，原有的源和目的地址配置等将丢失，需要重新配置。

     - 如果两端的封装模式相同，请执行步骤 2。
  2. 两端 tunnel 是否配置了 IP 地址、源地址和目的地址；两端是否互为源地址和目的地址

     确定 tunnel 两端封装模式一致后，检查两端的 tunnel 是否配置了 tunnel 的 IP 地址、源地址和目的地址，重点检查两端的 tunnel 是否互为源和目的地址。Tunnel 的源地址与目的地址唯一标识了一条隧道；如果不是互为源和目的地址，则就不能共同建立一条隧道。

     可以在 tunnel 接口视图下执行 **display this** 来检查两端 tunnel 的配置状态。Tunnel 接口配置信息中，两端应当互为源和目的地址

     - 如果 Tunnel 的接口配置信息中，两端没有互为源地址和目的地址，请在 Tunnel 接口视图下，重新配置 Tunnel 的源和目的地址。
     - 如果两端互为源地址和目的地址，请执行步骤 3。
  3. 检查 tunnel 源和目的地址之间是否存在路由

     确定两端 tunnel 接口的配置无误后，tunnel 的链路状态仍然是 Down，此时要检查 tunnel 的源地址所在的接口和目的地址所在的接口之间是否可达：

     - 如果两个接口不是直连的，检查这两个接口之间是否存在到对方的路由。
     - 如果将 tunnel 建立在直连的两个接口间，就不会存在路由的问题。

     使用 **display ip routing-table** 命令查看路由表。如果路由表正确，使用 **display fib** 命令查看转发表（FIB 表），即查看数据能否正确转发。FIB 表应与路由表一致。

     - 如果源和目的地址之间不存在到达对方的路由，请配置静态路由或者动态路由协议，使源和目的地址之间路由可达。
     - 如果源和目的地址之间存在到达对方的路由，但仍然无法 Ping 通，请执行步骤 4。
  4. 请收集如下信息，并联系华为技术支持工程师。
     - 上述步骤的执行结果。
     - 设备的配置文件、日志信息、告警信息。
- 两端 Tunnel 接口的网络层协议都 Up
  1. 检查两端 GRE Key 的配置是否一致

     在两端执行 **display interface tunnel** 命令，检查两端 tunnel 接口的 GRE Key 是否一致。正确的配置为：

版权所有 © 华为技术有限公司

- 或者两端都不配置 GRE Key；
- 或者两端配置相同的 key-number。

如果两端 Tunnel 接口 GRE Key 一致，但两端仍然 ping 不通对端，请执行步骤 2。

2. 检查两端 tunnel 接口的 IP 地址

   如果两端 tunnel 的状态都为 Up，但 **ping** 不通对端 tunnel 接口，需要检查两端 tunnel 接口的 IP 地址是否在同一网段：

   - 如果不在同一网段，则需要配置静态路由或动态路由，使本端设备有到对端 tunnel 接口 IP 地址的路由。
   - 如果 IP 地址在同一网段或者存在本端设备有到对端 tunnel 接口 IP 地址的路由，请执行步骤 3。

3. 请收集如下信息，并联系华为技术支持工程师。
   - 上述步骤的执行结果。
   - 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

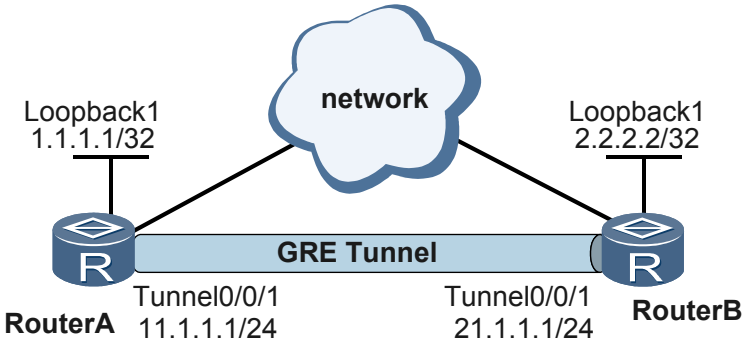
无

12.1.2 故障案例

两端 Tunnel 接口网络协议都 Up，但 ping 不通对端 Tunnel 接口

网络环境

图 12-3 GRE 本端 ping 不通对端 Tunnel 接口



版权所有 © 华为技术有限公司

GRE 两端 Tunnel 接口网络协议都 Up。但 RouterA 的 Tunnel0/0/1 与 RouterB 的 Tunnel0/0/1 之间无法互相 ping 通。

故障分析

出现此现象的可能原因有：

- 两端 GRE Key 的配置不一致
- 两端 tunnel 接口 IP 地址不在同一个网段且 tunnel 间没有可达路由

在两端执行 **display interface tunnel** *interface-number* 命令，检查两端 tunnel 接口的 GRE Key 是否一致。

```
<RouterA> display interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-03-08 16:58:30
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 11.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 1.1.1.1 (LoopBack1), destination 2.2.2.2
Tunnel protocol/transport GRE/IP, key 2
keepalive disabled
Checksumming of packets disabled
......
<RouterB> display interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-03-08 16:43:57
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 21.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 2.2.2.2 (LoopBack1), destination 1.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
......
```

显示结果可发现，RouterA 使能了 GRE Key，且配置 Key number 为 2；RouterB 没有使能 GRE Key。进行如下配置之一，使两端 GRE Key 的配置一致：

操作步骤

- 在 RouterA 上执行 **undo gre key** 命令去使能 GRE Key。
- 在 RouterB 上执行 **gre key 2** 使能 GRE Key。

  采用这两种方式之一修改后，Tunnel 接口两端可以相互 Ping 通。

----结束

案例总结

GRE 两端的 Tunnel 接口网络层协议为 Up，并不表明 GRE 隧道配置成功。还要使两端 GRE Key 的配置一致，且源端设备和目的端设备上都存在经过 Tunnel 转发的路由，即两端都有对端 Tunnel 接口 IP 地址的路由。

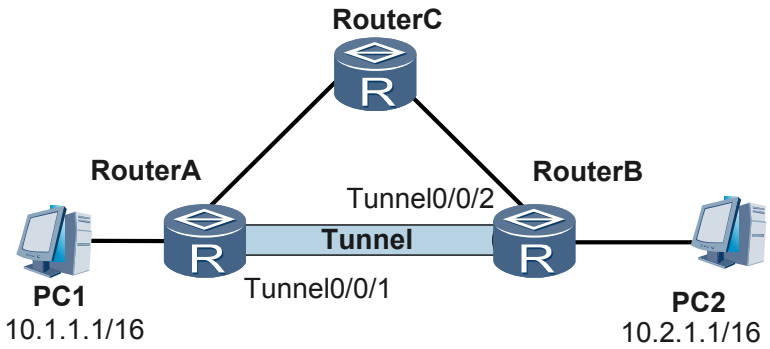
版权所有 © 华为技术有限公司

两端 Tunnel 接口可以 ping 通，PC 之间无法 ping 通

网络环境

如图 12-4 所示，Tunnel 两端接口配置正确且 Tunnel 两端可以 Ping 通，但 PC1 和 PC2 之间无法 Ping 通。

图 12-4 PC1 和 PC2 之间无法 Ping 通



故障分析

隧道配置正确，但 PC1 和 PC2 之间无法 Ping 通，可能原因有：

- RouterA 上没有到 PC2 的路由
- RouterB 上没有到 PC1 的路由
- PC1 未指定 RouterA 为自己的缺省网关
- PC2 未指定 RouterB 为自己的缺省网关

在 RouterA 和 RouterB 分别执行 **display ip routing-table** 命令，检查 RouterA 是否有经过 Tunnel0/0/1 接口到 10.2.0.0/16 的路由；在 RouterB 是否有经过 Tunnel0/0/2 接口到 10.1.0.0/16 的路由。

如果缺少相应的路由，在系统视图下使用 **ip route-static** 命令添加。以 RouterA 为例，配置如下：

```
[RouterA] ip route-static 10.2.0.0 255.255.0.0 tunnel 0/0/1
```

此时,如果 PC 之间仍无法 ping 通，则查看 PC1 是否指定 RouterA 为自己的缺省网关；然后查看 PC2 是否指定 RouterB 为自己的缺省网关。

操作步骤

步骤 1 检查 RouterA 是否有经过 Tunnel0/0/1 接口到 10.2.0.0/16 的路由。

步骤 2 检查 RouterB 是否有经过 Tunnel0/0/2 接口到 10.1.0.0/16 的路由。

步骤 3 检查 PC1 是否指定 RouterA 为自己的缺省网关。

步骤 4 检查 PC2 是否指定 RouterB 为自己的缺省网关。

----结束

版权所有 © 华为技术有限公司

案例总结

GRE 的两端 Tunnel 接口可以 ping 通后，要使 GRE 封装的报文正确转发，必须使源端设备和目的端设备上都存在经过 Tunnel 转发的路由。

12.2 IPSec 故障处理

12.2.1 采用 Manual 方式无法建立安全联盟的定位思路

常见原因

本类故障的常见原因主要包括：

- 链路故障
- 数据流未从指定接口转发
- IPSec 隧道两端的安全提议不一致
- IPSec 隧道两端的安全策略是否匹配：如设备本端地址和对端地址设置不正确、两端安全联盟参数不匹配
- 安全策略引用的 ACL 规则不互为镜像

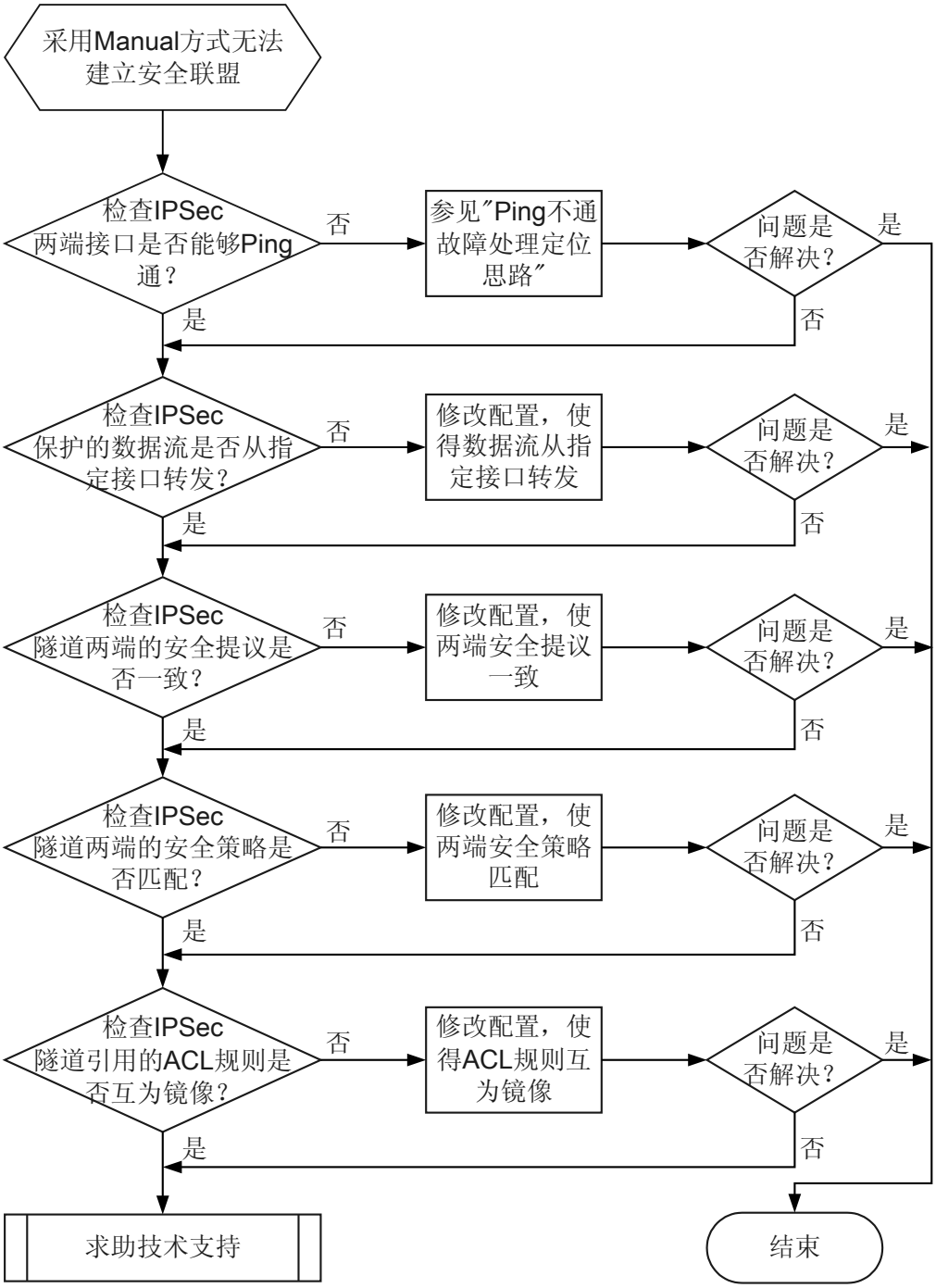
故障诊断流程

在用 Manual 方式配置 IPSec 后，发现 IPSec 无法对数据进行保护。

详细处理流程如图 12-5 所示。

版权所有 © 华为技术有限公司

图 12-5 采用 Manual 方式无法建立安全联盟故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查应用 IPSec 隧道两端接口是否能够 ping 通。

版权所有 © 华为技术有限公司

请先在 IPSec 隧道两端的 Router 接口上执行 **undo ipsec policy** 命令，将应用的 IPSec 策略删除。然后以一端接口 IP 地址为源 IP，**ping** 另一端的接口 IP 地址，查看是否可以 ping 通。

- 如果不能 ping 通，请参见 **7.1.1 Ping 不通问题的定位思路**检查两端的路由表中是否存在对端路由。
- 如果可以 ping 通，则说明隧道两端之间有可达路由。请恢复接口上配置的 IPSec 策略后，执行步骤 2。

步骤 2 检查 IPSec 隧道保护的数据流是否从指定接口转发。

应确保出方向的数据流通过应用了 IPSec 策略的接口发送。

具体检查方法如下：

- 在两端设备执行 **display ip routing-table** 命令，检查到对端的路由的下一跳可达的出接口是否为指定接口。如果不是指定接口，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IP 路由》修改路由配置。
- 在两端设备执行 **display arp** 命令，检查学习到的对端 IP 地址的 ARP 表项中的接口是否为指定接口。如果不是指定接口，请执行 **reset arp** 命令清除 ARP 映射表中的 ARP 项。

如果数据流是从指定接口转发，请执行步骤 3。

步骤 3 检查 IPSec 隧道两端的安全提议是否一致。

分别在两端设备上执行 **display ipsec proposal** 命令，查看两端 IPSec 安全提议的配置是否保持一致。具体检查项如下表所示：

检查项	检查标准和后续操作方法
IPsec Proposal Name	检查两端 IPSec 安全策略中绑定的提议的是否一致，如果不一致，请执行 **ipsec proposal** 命令修改配置。
Encapsulation Mode	检查提议采用的模式是否一致，如果不一致，请执行 **encapsulation-mode** { **transport** | **tunnel** } 命令修改配置。
Transform	检查提议采用的安全协议是否一致，如果不一致，请执行 **transform** { **ah** | **esp** | **ah-esp** }命令修改配置。
AH Protocol	检查 AH 协议采用的认证算法是否一致，如果不一致，请执行 **ah authentication-algorithm** { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512**} 命令修改配置。
ESP Protocol	检查 ESP 协议采用的认证算法和加密算法是否一致，如果不一致，请执行 **esp authentication-algorithm** [**md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512**]命令修改认证算法，执行 **esp encryption-algorithm** [**3des** | **des** | **aes-128** | **aes-192** | **aes-256**]命令修改加密算法。

如果两端的 IPSec 安全提议一致，请执行步骤 4。

步骤 4 检查 IPSec 隧道两端的安全策略是否匹配。

分别在两端设备上执行 **display ipsec policy** 命令，两端 IPSec 安全策略的配置应该保持匹配。具体检查项如下表所示：

版权所有 © 华为技术有限公司

检查项	检查标准及后续操作方法
tunnel local address tunnel remote address	查看设备本端地址和对端地址设置是否正确。如果不正确，请执行 **tunnel local** 命令修改本端地址，执行 **tunnel remote** 命令修改对端地址。
Inbound/ Outbound AH/ESP setting	查看两端安全联盟参数 **SPI**、**string-key**、**authentication-hex** 和 **encryption-hex** 配置是否匹配，即本端的入方向安全联盟参数必须和对端的出方向安全联盟参数一样；本端的出方向安全联盟参数必须和对端的入方向安全联盟参数一样。如果参数不匹配，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》修改配置。

如果两端的 IPSec 安全策略匹配，请执行步骤 5。

步骤 5 检查 IPSec 隧道两端安全策略引用的 ACL 规则是否互为镜像。

在两端 Router 上分别执行 **display acl** 命令，如果两端设备作如下显示，说明两端安全策略引用的 ACL 互相镜像。

RouterA 的 ACL 配置信息。

```
<RouterA>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

RouterB 的 ACL 配置信息。

```
<RouterB>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

- 如果不互为镜像，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》修改配置。
- 如果配置正确，请执行下面的步骤 6。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

12.2.2 采用 IKE 方式无法建立安全联盟的定位思路

常见原因

本类故障的常见原因主要包括：

- 链路故障
- 数据流未从指定接口转发
- 数据流不能命中 ACL 规则
- IPSec 隧道两端的安全提议不一致
- IPSec 隧道两端的安全策略是否匹配：如 IPSec 协商模式不一致、PFS 配置不一致
- 安全策略引用的 ACL 规则不互为镜像
- 两端对等体的 IKE 安全提议不一致
- IKE peer 配置不正确：如 IKE 协商模式不相同、IKE 版本不相同、IKE peer 的 IP 地址不匹配、IKE peer 的对端名称不匹配

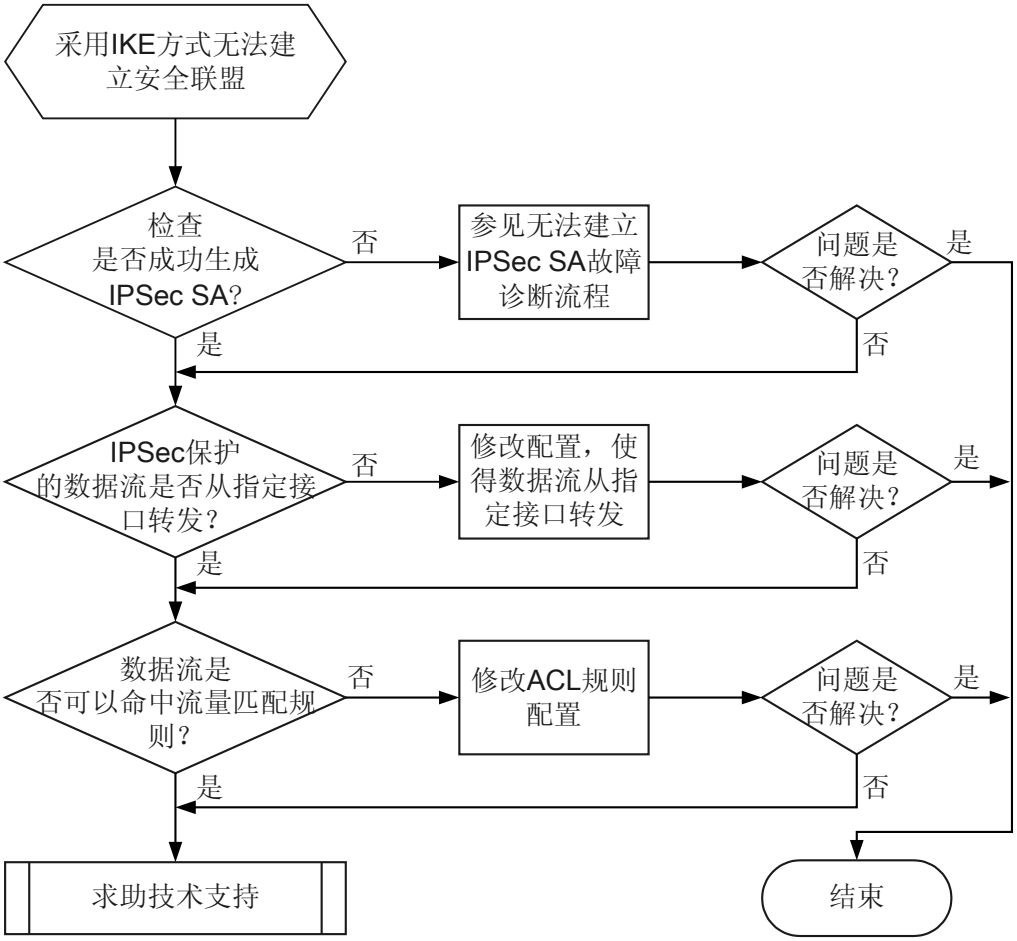
故障诊断流程

在采用 IKE 方式配置 IPSec 后，发现 IPSec 无法对数据进行保护。

详细处理流程如**图 12-6**、**图 12-7** 和**图 12-8** 所示。

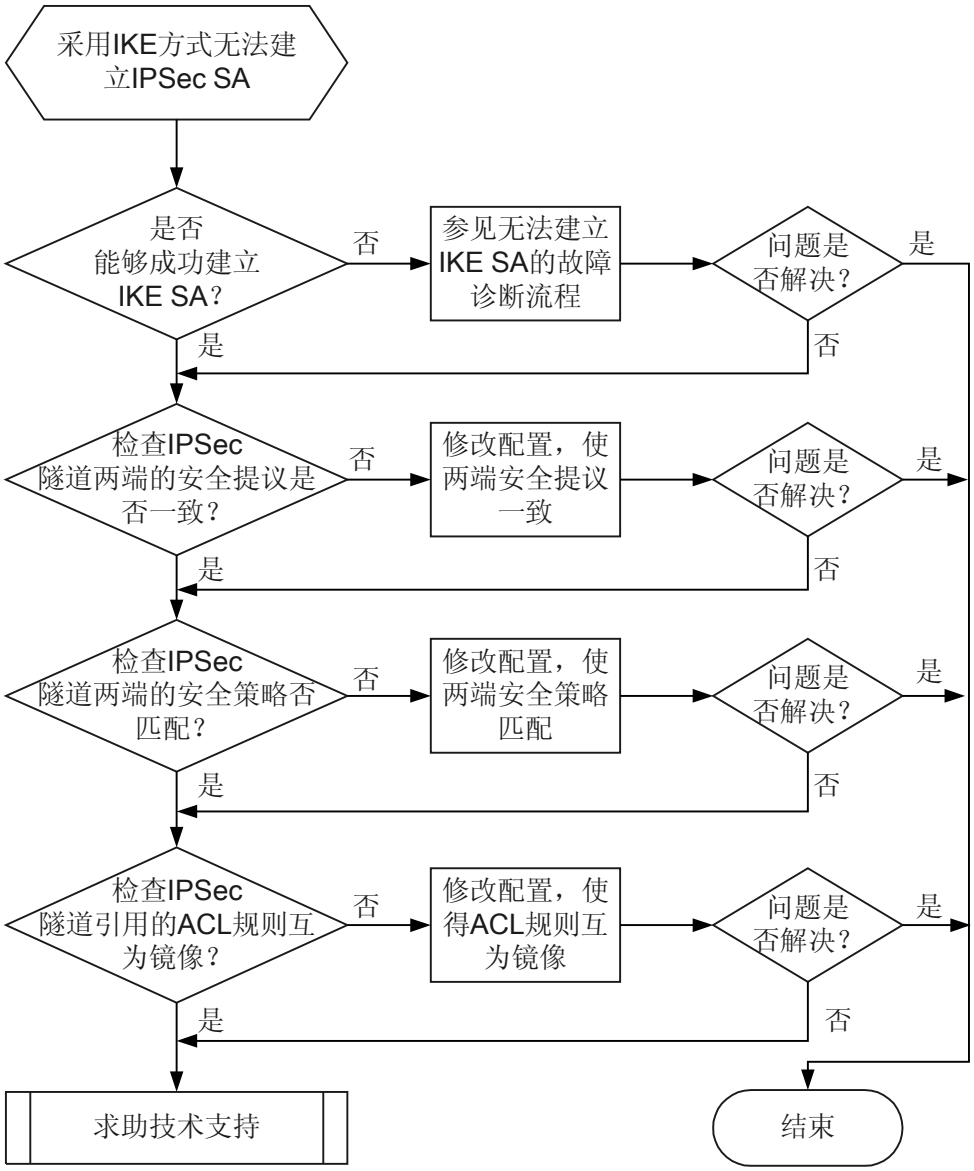
版权所有 © 华为技术有限公司

图 12-6 采用 IKE 方式无法建立安全联盟的故障诊断流程图



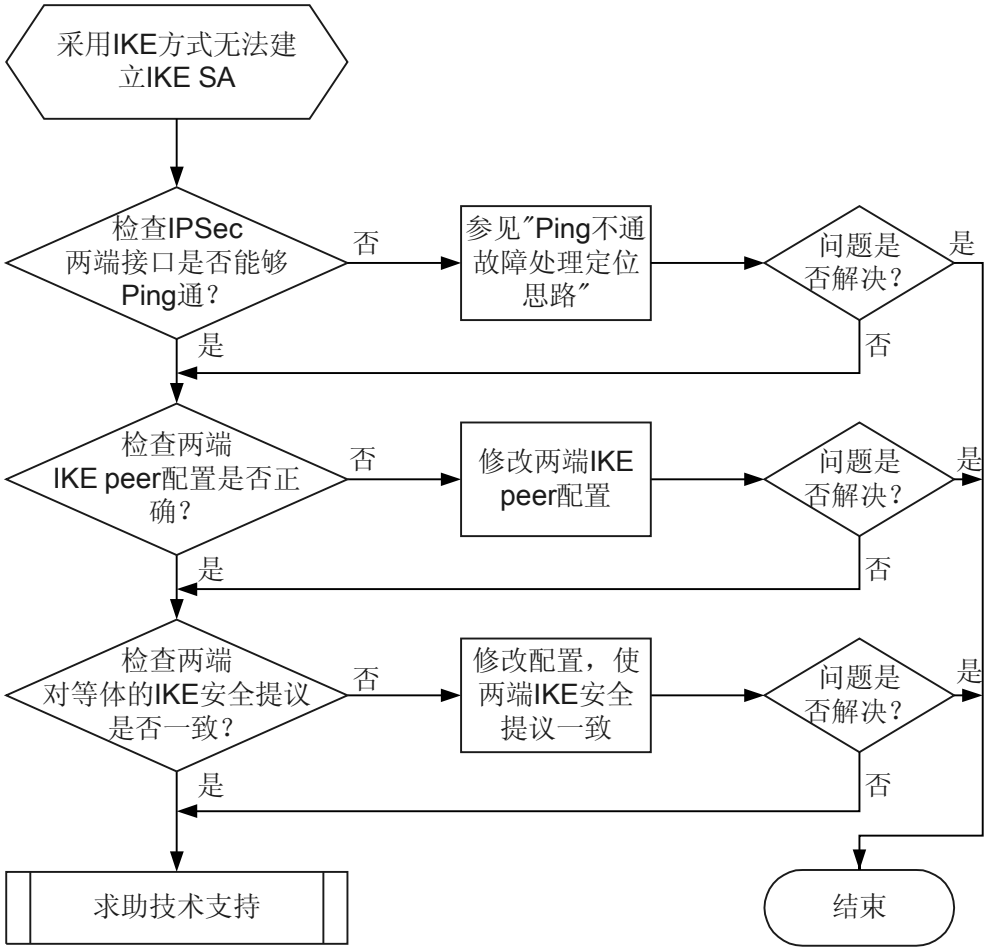
版权所有 © 华为技术有限公司

图 12-7 采用 IKE 方式无法建立 IPSec SA 的故障诊断流程图



版权所有 © 华为技术有限公司

图 12-8 采用 IKE 方式无法建立 IKE SA 的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查是否成功建立生成 IPSec SA 和 IKE SA。

执行 **display ike sa** 命令，通过查看 **Peer**、**Flag** 和 **Phase** 字段可知哪些对等体建立了哪个阶段的 SA。显示信息如下可知，IP 地址为 30.0.0.1 的 Peer 第一阶段协商建立了 IKE SA，第二阶段协商建立了 IPSec SA。

```
<RouterA>display ike sa
    Conn-ID  Peer            VPN   Flag(s)                 Phase
-------------------------------------------------------------------
    397      30.0.0.1        0     RD                      2
    367      30.0.0.1        0     RD                      1

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
```

说明

如果两端配置的 IKE 版本是 v1，使用命令 **display ike sa**。如果两端配置的 IKE 版本是 v2，使用命令 **display ike sa v2**。

版权所有 © 华为技术有限公司

- 如果成功建立了 IPSec SA 和 IKE SA，请执行步骤 2。
- 如果未成功建立 IPSec SA，但是成功建立了 IKE SA，请执行步骤 4。
- 如果未成功建立 IKE SA，请执行步骤 8。

步骤 2 检查 IPSec 隧道保护的数据流是否从指定接口转发。

应确保出方向的数据流通过应用了 IPSec 策略的接口发送。

具体检查方法如下：

- 在两端设备执行 **display ip routing-table** 命令，检查到对端的路由的下一跳可达的出接口是否为指定接口。如果不是指定接口，请参考《Huawei AR2200-S 系列 企业路由器 配置指南-IP 路由》修改路由配置。
- 在两端设备执行 **display arp** 命令，检查学习到的对端 IP 地址的 ARP 表项中的接口是否为指定接口。如果不是指定接口，请执行 **reset arp** 命令清除 ARP 映射表中的 ARP 项。

如果数据流是从指定接口转发，请执行步骤 3。

步骤 3 检查数据流是否可以命中流量匹配规则。

分析数据流量的源、目的 IP，源和目的端口号等信息，检查流量是否能够匹配 IPSec 策略中引用的 ACL 规则。

- 如果数据流不能命中流量匹配规则，则报文就进入不了 IPSec 隧道，而被直接转发。请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》进行修改流量匹配规则。
- 如果数据流可以命中，请执行步骤 10。

步骤 4 检查 IPSec 隧道两端的安全提议是否一致。

分别在两端设备上执行 **display ipsec proposal** 命令，查看两端 IPSec 安全提议的配置是否保持一致。具体检查项如下表所示：

检查项	检查标准和后续操作方法
IPsec Proposal Name	检查两端 IPSec 安全策略中绑定的提议的是否一致，如果不一致，请执行 **ipsec proposal** 命令修改配置。
Encapsulation Mode	检查提议采用的模式是否一致，如果不一致，请执行 **encapsulation-mode** { **transport** | **tunnel** } 命令修改配置。
Transform	检查提议采用的安全协议是否一致，如果不一致，请执行 **transform** { **ah** | **esp** | **ah-esp** }命令修改配置。
AH Protocol	检查 AH 协议采用的认证算法是否一致，如果不一致，请执行 **ah authentication-algorithm** { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** } 命令修改配置。
ESP Protocol	检查 ESP 协议采用的认证算法和加密算法是否一致，如果不一致，请执行 **esp authentication-algorithm** [**md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512**]命令修改认证算法，执行 **esp encryption-algorithm** [**3des** | **des** | **aes-128** | **aes-192** | **aes-256**]命令修改加密算法。

如果两端的 IPSec 安全提议一致，请执行步骤 5。

版权所有 © 华为技术有限公司

步骤 5 检查 IPsec 隧道两端的安全策略是否匹配。

请查看下列检查项：

检查项	判断标准及后续操作步骤
IPSec 协商模式	执行 **display ipsec policy brief** 命令查看 **Mode** 字段，两端的协商模式必须保持一致，如果不一致，请执行 **ipsec policy isakmp** 命令修改配置。
DH（Diffie-Hellman）组	如果本端指定了 PFS，对端在发起协商时必须是 PFS 交换，即本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。执行 **display ipsec policy** 命令查看 **Perfect Forward Secrecy** 字段，如果两端配置不一致，请执行 **pfs** { **dh-group1** | **dh-group2** } 修改配置。

如果两端的安全策略匹配，请执行步骤 6。

步骤 6 检查 IPSec 隧道两端安全策略引用的 ACL 是否互为镜像。

在两端 Router 上分别执行 **display acl** 命令，如果两端设备作如下显示，说明两端安全策略引用的 ACL 互相镜像。

RouterA 的 ACL 配置信息。

```
<RouterA>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

RouterB 的 ACL 配置信息。

```
<RouterB>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

- 如果不互为镜像，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》修改配置。
- 如果配置正确，请执行下面的步骤 2。

步骤 7 检查应用 IPSec 隧道两端接口是否能够 ping 通。

请先在 IPSec 隧道两端的 Router 接口上执行 **undo ipsec policy** 命令，将引用的 IPSec 策略删除。然后以一端接口 IP 地址为源 IP，**ping** 另一端的接口 IP 地址，查看是否可以 ping 通。

- 如果不能 ping 通，请参见 **7.1.1 Ping 不通问题的定位思路**检查两端的路由表中是否存在对端路由。
- 如果可以 ping 通，则说明隧道两端之间有可达路由。请恢复接口上配置的 IPSec 策略后，执行步骤 8。

步骤 8 检查 IKE peer 配置是否正确。

执行 **display ike peer** 命令，检查项目如下图所示：

检查项	判断方法及后续操作步骤
Exchange mode	第一阶段的协商模式即 IKE 协商模式必须相同，如果不相同，请执行 **exchange-mode** { **main** | **aggressive** }命令修改配置。

版权所有 © 华为技术有限公司

检查项	判断方法及后续操作步骤
Negotiated IKE version	IKE 版本必须相同，如果不相同，请执行 **ike peer** 命令修改配置。
Peer ip address Local ip address	隧道一端的 IKE peer 的 **Peer ip address** 应该等于隧道另一端的 IKE peer 的 **Local ip address**。隧道一端的 IKE peer 的 **Local ip address** 应该等于隧道另一端的 IKE peer 的 **Peer ip address**。如果不匹配，请执行 **local-address** 命令修改 IKE 本端 IP 地址，执行 **remote-address** 命令修改 IKE peer 对端的 IP 地址。
remote-name	对端名称必须与对端的本地名称一致，如果不匹配，请执行 **remote-name** 命令来修改配置。 **说明** 以下情况会使用对端名称: ● IKEv1 版本时，协商模式为野蛮模式下且使用名字认证的情况下 ● IKEv2 版本时，当远端的 peer IKE 的 ID 类型为 name 的情况下

如果 IKE peer 配置正确，请执行步骤 9。

步骤 9 检查 IPSec 隧道两端对等体的 IKE 安全提议是否一致。

分别在两端设备上执行 **display ike proposal** 命令，两端 IKE 安全提议的配置应该保持一致。

- 如果两端的 IKE 安全提议不一致，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》重新配置 IKE 安全提议。
- 如果两端的 IKE 安全提议一致，请执行步骤 2。

说明

如果将认证方式设置为预共享密钥认证方式，则需要为每个对端配置预共享密钥，且建立安全连接的两个对端的预共享密钥必须一致，如果两端不一致，请执行 **pre-shared-key** 命令修改 pre-shared key 认证方法的认证字。

步骤 10 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

12.2.3 采用安全策略模板配置 IPSec 失败的定位思路

版权所有 © 华为技术有限公司

常见原因

本类故障的常见原因主要包括：

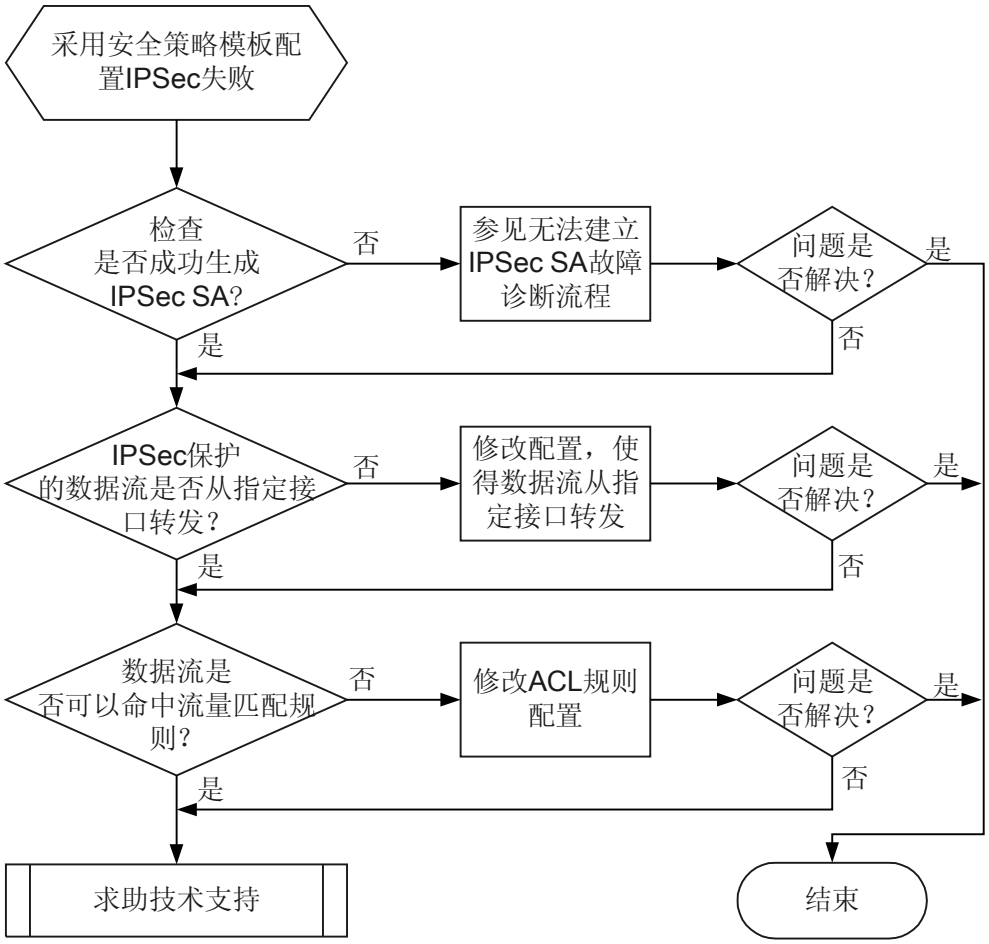
- 链路故障
- 数据流未从指定接口转发
- 数据流不能命中 ACL 规则
- IPSec 隧道两端的安全提议不一致
- IPSec 安全策略协商不是由对端发起
- IPSec 隧道两端的安全策略是否匹配：如 PFS 配置不一致
- 安全策略引用的 ACL 规则不互为镜像
- 两端对等体的 IKE 安全提议不一致
- IKE peer 配置不正确：如 IKE 协商模式不相同、IKE 版本不相同、IKE peer 的 IP 地址不匹配、IKE peer 的对端名称不匹配

故障诊断流程

在采用安全策略模板配置 IPSec 后，发现 IPSec 无法对数据进行保护。

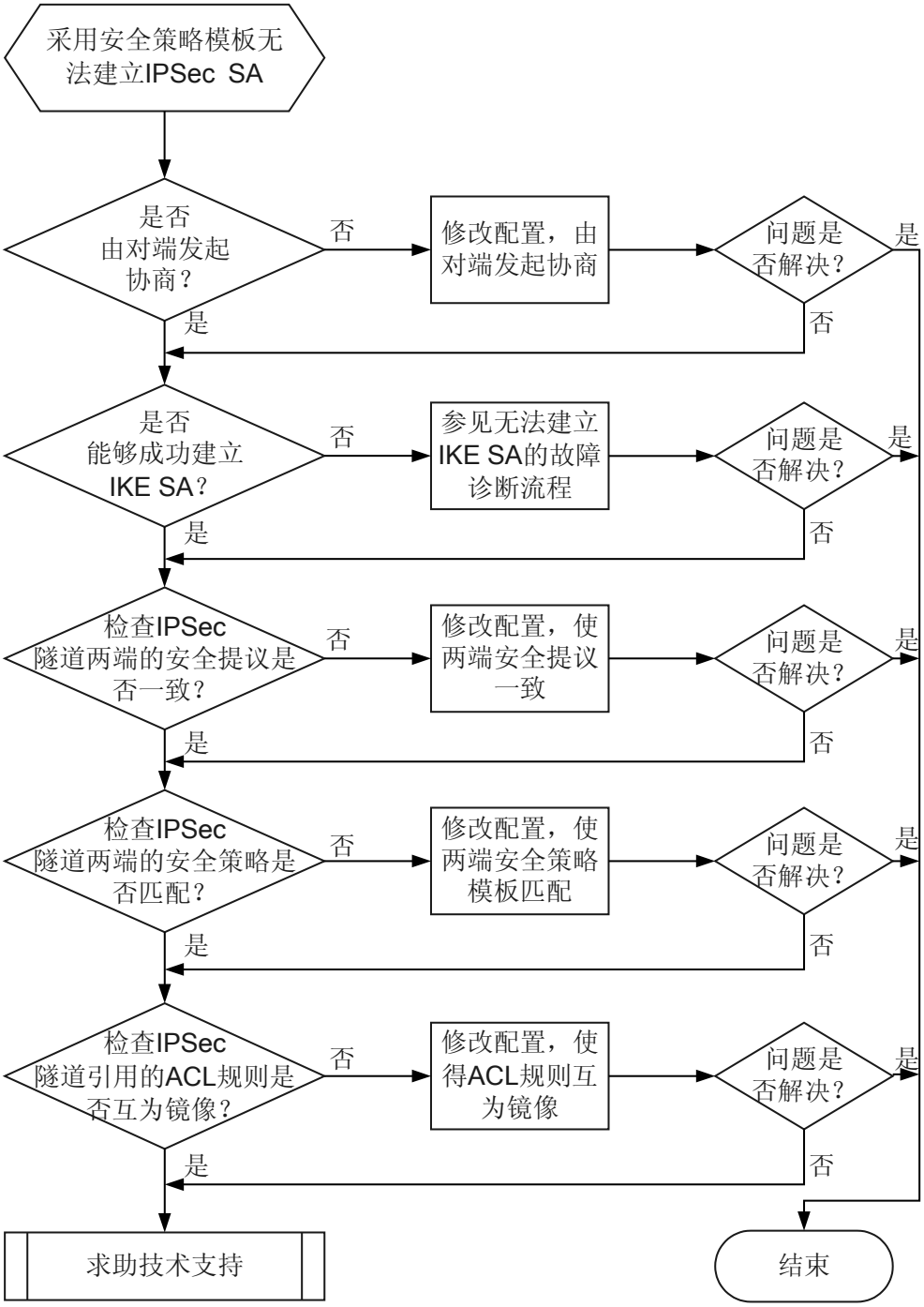
详细处理流程如图 12-9 所示。

图 12-9 采用安全策略模板配置 IPSec 失败故障诊断流程图



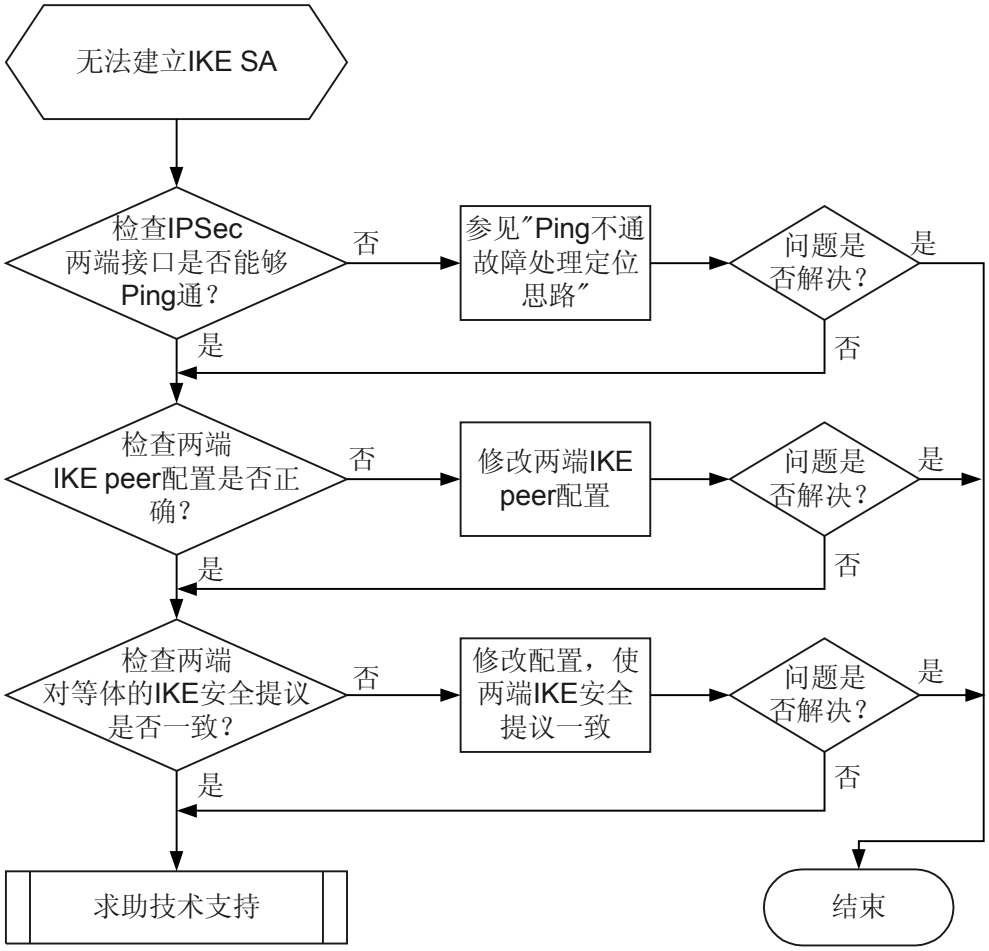
版权所有 © 华为技术有限公司

图 12-10 采用安全策略模板无法建立 IPSec SA 故障诊断流程图



版权所有 © 华为技术有限公司

图 12-11 采用安全策略模板无法建立 IKE SA 故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查是否成功建立生成 IPSec SA 和 IKE SA。

执行 **display ike sa** 命令，通过查看 **Peer**、**Flag** 和 **Phase** 字段可知哪些对等体建立了哪个阶段的 SA。显示信息如下可知，IP 地址为 30.0.0.1 的 Peer 第一阶段协商建立了 IKE SA，第二阶段协商建立了 IPSec SA。

```
<RouterA>display ike sa
    Conn-ID  Peer            VPN   Flag(s)                 Phase
-------------------------------------------------------------------
    397      30.0.0.1        0     RD                      2
    367      30.0.0.1        0     RD                      1

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
```

说明

如果两端配置的 IKE 版本是 v1，使用命令 **display ike sa**。如果两端配置的 IKE 版本是 v2，使用命令 **display ike sa v2**。

版权所有 © 华为技术有限公司

- 如果成功建立了 IPSec SA 和 IKE SA，请执行步骤 2。
- 如果未成功建立 IPSec SA，但是成功建立了 IKE SA，请执行步骤 4。
- 如果未成功建立 IKE SA，请执行步骤 6。

步骤 2 检查 IPSec 隧道保护的数据流是否从指定接口转发。

应确保出方向的数据流通过应用了 IPSec 策略的接口发送。

具体检查方法如下：

- 在两端设备执行 **display ip routing-table** 命令，检查到对端的路由的下一跳可达的出接口是否为指定接口。如果不是指定接口，请参考《Huawei AR2200-S 系列 企业路由器 配置指南-IP 路由》修改路由配置。
- 在两端设备执行 **display arp** 命令，检查学习到的对端 IP 地址的 ARP 表项中的接口是否为指定接口。如果不是指定接口，请执行 **reset arp** 命令清除 ARP 映射表中的 ARP 项。

如果数据流是从指定接口转发，请执行步骤 3。

步骤 3 检查数据流是否可以命中流量匹配规则。

分析数据流量的源、目的 IP，源和目的端口号等信息，检查流量是否能够匹配 IPSec 策略中引用的 ACL 规则。

- 如果数据流不能命中流量匹配规则，报文就进入不了 IPSec 隧道，而被直接转发。请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》进行修改对端设备的 ACL 规则。
- 如果数据流可以命中，请执行步骤 10。

步骤 4 检查 IPSec 隧道两端的安全提议是否一致。

分别在两端设备上执行 **display ipsec proposal** 命令，查看两端 IPSec 安全提议的配置是否保持一致。具体检查项如下表所示：

检查项	检查标准和后续操作方法
IPsec Proposal Name	检查两端 IPSec 安全策略中绑定的提议的是否一致.，如果不一致，请执行 **ipsec proposal** 命令修改配置。
Encapsulation Mode	检查提议采用的模式是否一致，如果不一致，请执行 **encapsulation-mode** { **transport** | **tunnel** } 命令修改配置。
Transform	检查提议采用的安全协议是否一致，如果不一致，请执行 **transform** { **ah** | **esp** | **ah-esp** }命令修改配置。
AH Protocol	检查 AH 协议采用的认证算法是否一致，如果不一致，请执行 **ah authentication-algorithm** { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** } 命令修改配置。
ESP Protocol	检查 ESP 协议采用的认证算法和加密算法是否一致，如果不一致，请执行 **esp authentication-algorithm** [**md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512**]命令修改认证算法，执行 **esp encryption-algorithm** [**3des** | **des** | **aes-128** | **aes-192** | **aes-256**]命令修改加密算法。

如果两端的 IPSec 安全提议一致，请执行步骤 5。

版权所有 © 华为技术有限公司

步骤 5 检查对端安全策略的协商方式是否为自动协商。

在对端设备上执行 **display ipsec policy** 命令，查看 **SA trigger mode** 字段是否为 **Automatic**。由于本端配置的安全策略为安全策略模板方式，不会主动发起协商，必须对端发起协商。而基于流量触发方式的也不会主动发起协商，因此对端的触发方式必须为自动触发方式。

- 如果不是自动发方式，请执行 **sa trigger-mode auto** 命令修改。
- 如果是，请执行步骤 6。

步骤 6 检查隧道两端的 IPSec 安全策略是否匹配。

请查看下列检查项：

检查项	判断标准及后续操作步骤
两端 ACL 规则是否为镜像	**说明** 安全策略模板方式下可以选择配置或不配置 ACL 规则，如果配置了 ACL 规则，请保证 ACL 规则的匹配。 建议安全策略模板下不配置 ACL 规则。 如果安全模板上配置了 ACL 规则，在两端 Router 上分别执行 **display acl** 命令，如果两端设备作如下显示，说明两端安全策略引用的 ACL 互相镜像 # RouterA 的 ACL 配置信息。 <RouterA>**display acl 3101** Advanced ACL 3101, 1 rule Acl's step is 5 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 # RouterB 的 ACL 配置信息。 <RouterB>**display acl 3101** Advanced ACL 3101, 1 rule Acl's step is 5 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 如果 ACL 规则不匹配，请修改对端 ACL 规则。
DH 组 (Diffie-Hellman)	如果本端指定了 PFS，对端在发起协商时必须是 PFS 交换，即本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。执行 **display ipsec policy** 命令查看 **Perfect Forward Secrecy** 字段，如果两端配置不一致，请执行 **pfs** { **dh-group1** | **dh-group2** } 修改配置。

如果两端的安全策略模板匹配，请执行步骤 2。

步骤 7 检查应用 IPSec 隧道两端接口是否能够 ping 通。

请先在 IPSec 隧道两端的 Router 接口上执行 **undo ipsec policy** 命令，将引用的 IPSec 策略删除。然后以一端接口 IP 地址为源 IP，**ping** 另一端的接口 IP 地址，查看是否可以 ping 通。

- 如果不能 ping 通，请参见 **7.1.1 Ping 不通问题的定位思路**检查两端的路由表中是否存在对端路由。
- 如果可以 ping 通，则说明隧道两端之间有可达路由。请恢复接口上配置的 IPSec 策略后，执行步骤 8。

步骤 8 检查 IKE peer 配置是否正确。

执行 **display ike peer** 命令，检查项目如下图所示：

版权所有 © 华为技术有限公司

检查项	判断方法及后续操作步骤
Exchange mode	第一阶段的协商模式即 IKE 协商模式必须相同，如果不相同，请执行 **exchange-mode** { **main** | **aggressive** }命令修改配置。
Negotiated IKE version	IKE 版本必须相同，如果不相同，请执行 **ike peer** 命令修改配置。
Peer ip address Local ip address	隧道一端的 IKE peer 的 **Peer ip address** 应该等于隧道另一端的 IKE peer 的 **Local ip address**。隧道一端的 IKE peer 的 **Local ip address** 应该等于隧道另一端的 IKE peer 的 **Peer ip address**。如果不匹配，请执行 **local-address** 命令修改 IKE 本端 IP 地址。
remote-name	对端名称必须与对端的本地名称一致，如果不匹配，请执行 **remote-name** 命令来修改配置。 **说明** 以下情况会使用对端名称: ● IKEv1 版本时，协商模式为野蛮模式下且使用名字认证的情况下 ● IKEv2 版本时，当远端的 peer IKE 的 ID 类型为 name 的情况下

如果 IKE peer 配置正确，请执行步骤 9。

步骤 9 检查 IPSec 隧道两端对等体的 IKE 安全提议是否一致。

分别在两端设备上执行 **display ike proposal** 命令，两端 IKE 安全提议的配置应该保持一致。

- 如果两端的 IKE 安全提议不一致，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》重新配置 IKE 安全提议。
- 如果两端的 IKE 安全提议一致，请执行步骤 2。

说明

如果将认证方式设置为预共享密钥认证方式，则需要为每个对端配置预共享密钥，且建立安全连接的两个对端的预共享密钥必须一致，如果两端不一致，请执行 **pre-shared-key** 命令修改 pre-shared key 认证方法的认证字。

步骤 10 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

12.2.4 IPSec 的 NAT 穿越的定位思路

常见原因

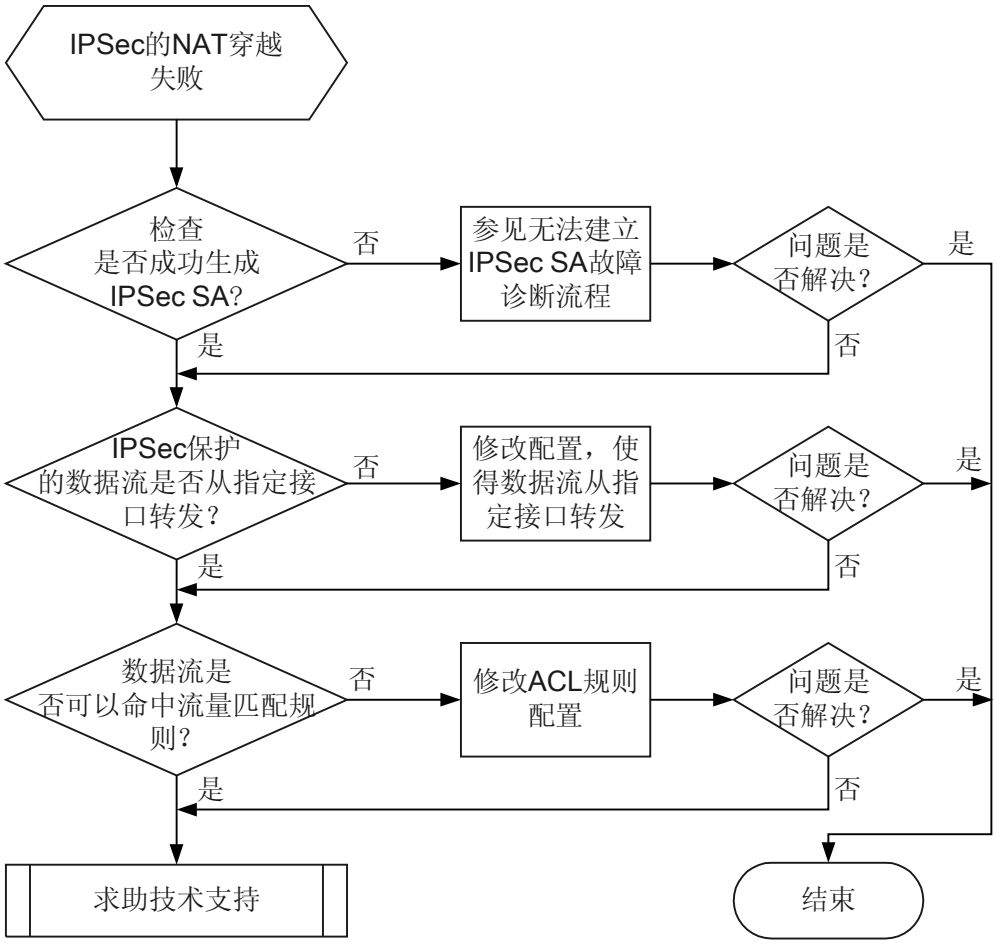
本类故障的常见原因主要包括：

- 链路故障
- 数据流未从指定接口转发
- 数据流不能命中 ACL 规则
- IPSec 隧道两端的安全提议不一致或是提议采用的安全协议不为 ESP
- IPSec 隧道两端的安全策略是否匹配：如 IPSec 协商模式不一致、PFS 配置不一致
- 安全策略引用的 ACL 规则不互为镜像
- 两端对等体的 IKE 安全提议不一致
- IKE peer 配置不正确：如 IKE 协商模式不是野蛮模式、IKE 版本不相同、IKE peer 的 IP 地址不匹配、IKE peer 的对端名称不匹配、未使能 NAT 穿越功能、本地 ID 类型不为 name

故障诊断流程

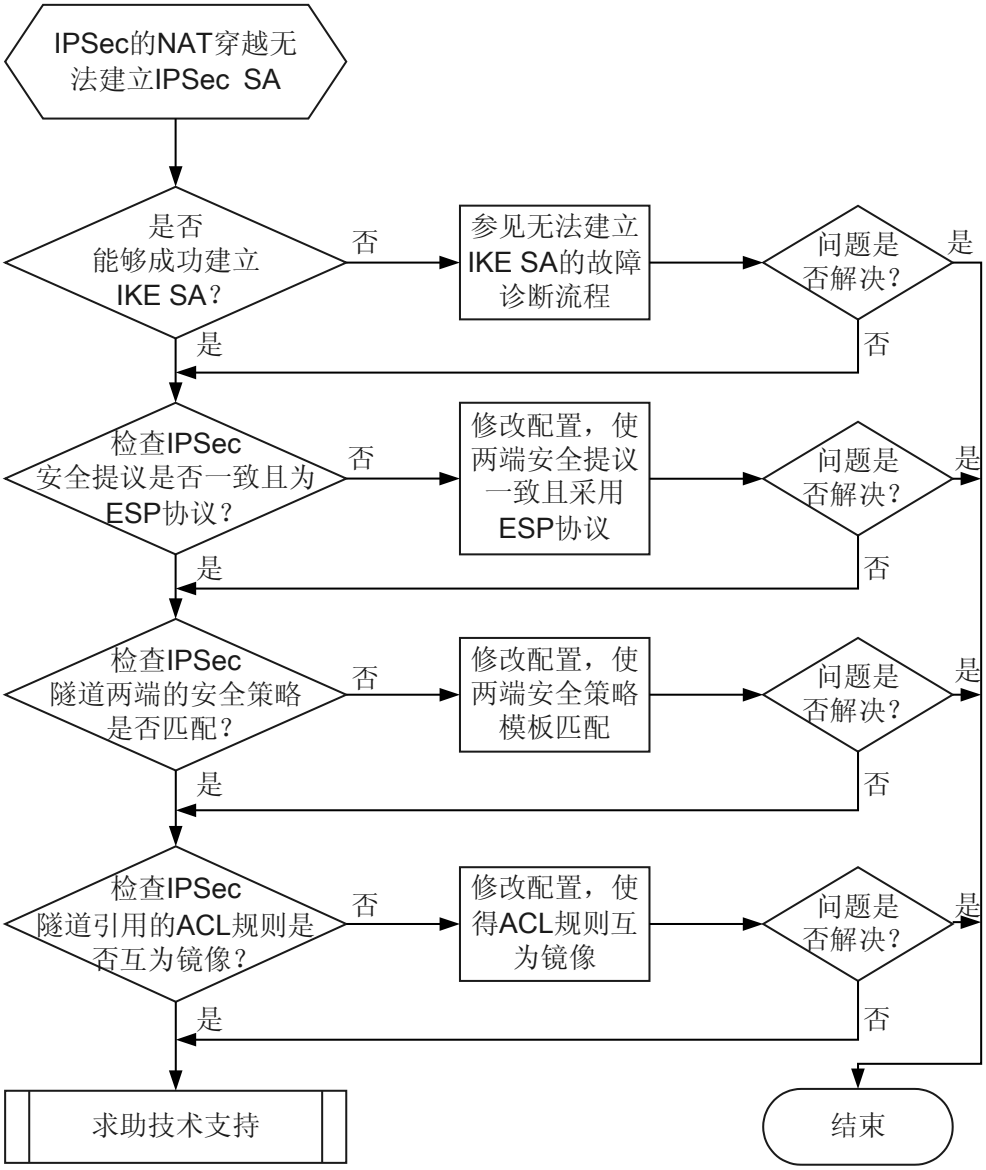
详细处理流程如图 12-12 所示。

图 12-12 IPSec 的 NAT 穿越的定位思路故障诊断流程图



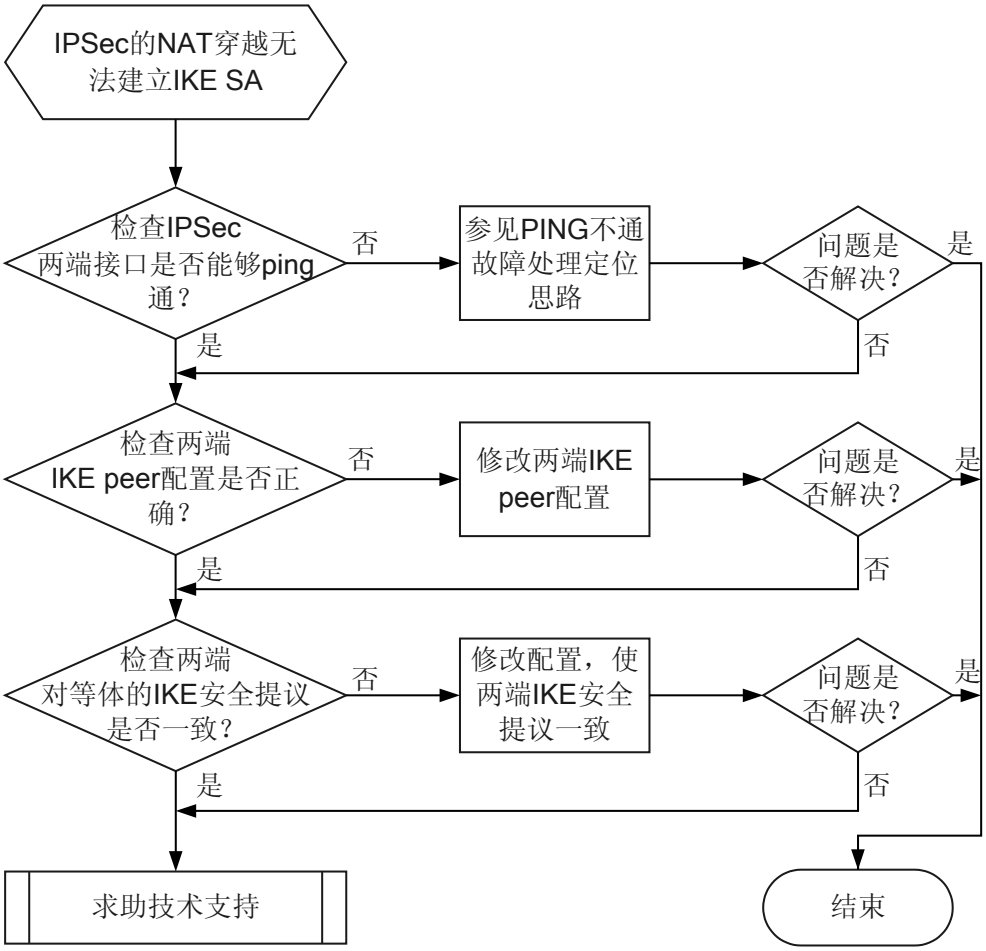
版权所有 © 华为技术有限公司

图 12-13 IPSec 的 NAT 穿越的定位思路故障诊断流程图



版权所有 © 华为技术有限公司

图 12-14 IPSec 的 NAT 穿越的定位思路故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查是否成功建立生成 IPSec SA 和 IKE SA。

执行 **display ike sa** 命令，通过查看 **Peer**、**Flag** 和 **Phase** 字段可知哪些对等体建立了哪个阶段的 SA。显示信息如下可知，IP 地址为 30.0.0.1 的 Peer 第一阶段协商建立了 IKE SA，第二阶段协商建立了 IPSec SA。

```
<Router A>display ike sa
    Conn-ID  Peer            VPN   Flag(s)                 Phase
-------------------------------------------------------------------
    397      30.0.0.1        0     RD                      2
    367      30.0.0.1        0     RD                      1

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
```

说明

如果两端配置的 IKE 版本是 v1，使用命令 **display ike sa**。如果两端配置的 IKE 版本是 v2，使用命令 **display ike sa v2**。

版权所有 © 华为技术有限公司

- 如果成功建立了 IPSec SA 和 IKE SA，请执行步骤 2。
- 如果未成功建立 IPSec SA，但是成功建立了 IKE SA，请执行步骤 4。
- 如果未成功建立 IKE SA，请执行步骤 8。

步骤 2 检查 IPSec 隧道保护的数据流是否从指定接口转发。

应确保出方向的数据流通过应用了 IPSec 策略的接口发送。

具体检查方法如下：

- 在两端设备执行 **display ip routing-table** 命令，检查到对端的路由的下一跳可达的出接口是否为指定接口。如果不是指定接口，请参考《Huawei AR2200-S 系列 企业路由器 配置指南-IP 路由》修改路由配置。
- 在两端设备执行 **display arp** 命令，检查学习到的对端 IP 地址的 ARP 表项中的接口是否为指定接口。如果不是指定接口，请执行 **reset arp** 命令清除 ARP 映射表中的 ARP 项。

如果数据流是从指定接口转发，请执行步骤 3。

步骤 3 检查数据流是否可以命中流量匹配规则。

分析数据流量的源 IP 地址和目的 IP 地址，源和目的端口号等信息，检查流量是否能够匹配 IPSec 策略中引用的 ACL 规则。

- 如果数据流不能命中流量匹配规则，报文就进入不了 IPSec 隧道，而被直接转发。请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》进行修改流量匹配规则。
- 如果数据流可以命中，请执行步骤 10。

步骤 4 检查 IPSec 隧道两端的安全提议是否一致且提议采用的安全协议为 ESP。

分别在两端设备上执行 **display ipsec proposal** 命令，查看两端 IPSec 安全提议的配置是否保持一致。具体检查项如下表所示：

检查项	检查标准和后续操作方法
IPsec Proposal Name	检查两端 IPSec 安全策略中绑定的提议的是否一致.，如果不一致，请执行 **ipsec proposal** 命令修改配置。
Encapsulation Mode	检查提议采用的模式是否一致，如果不一致，请执行 **encapsulation-mode** { **transport** | **tunnel** } 命令修改配置。
Transform	检查提议采用的安全协议是否一致，如果不一致，请执行 **transform esp** 命令修改配置。
ESP Protocol	检查 ESP 协议采用的认证算法和加密算法是否一致，如果不一致，请执行 **ah authentication-algorithm** { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }命令修改认证算法，执行 **esp encryption-algorithm** [**3des** | **des** | **aes-128** | **aes-192** | **aes-256**]命令修改加密算法。

如果两端的 IPSec 安全提议一致且提议采用的安全协议为 ESP，请执行步骤 5。

步骤 5 检查 IPsec 隧道两端的安全策略是否匹配。

版权所有 © 华为技术有限公司

说明

IPSec 穿越 NAT 的如果采用的是安全策略模板方式，在这种情况下可以选择配置或不配置 ACL 规则，如果配置了 ACL 规则，请保证 ACL 规则的匹配。

建议安全策略模板下不配置 ACL 规则。

请查看下列检查项：

检查项	判断标准及后续操作步骤
IPSec 协商模式	执行 **display ipsec policy brief** 命令查看 **Mode** 字段，两端的协商模式必须保持一致，如果不一致，请执行 **ipsec policy isakmp** 命令修改配置。
DH（Diffie-Hellman）组	如果本端指定了 PFS，对端在发起协商时必须是 PFS 交换，即本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。执行 **display ipsec policy** 命令查看 **Perfect Forward Secrecy** 字段，如果两端配置不一致，请执行 **pfs** { **dh-group1** | **dh-group2** } 修改配置。

如果两端的安全策略匹配，请执行步骤 6。

步骤 6 检查 IPSec 隧道两端安全策略引用的 ACL 是否互为镜像。

在两端 Router 上分别执行 **display acl** 命令，如果两端设备作如下显示，说明两端安全策略引用的 ACL 互相镜像。

RouterA 的 ACL 配置信息。

```
<RouterA>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

RouterB 的 ACL 配置信息。

```
<RouterB>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.
```

- 如果不互为镜像，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》修改配置。
- 如果配置正确，请执行下面的步骤 2。

步骤 7 检查应用 IPSec 隧道两端接口是否能够 ping 通。

请先在 IPSec 隧道两端的 Router 接口上执行 **undo ipsec policy** 命令，将引用的 IPSec 策略删除。然后以一端接口 IP 地址为源 IP，**ping** 另一端的接口 IP 地址，查看是否可以 ping 通。

- 如果不能 ping 通，请参见 **7.1.1 Ping 不通问题的定位思路**检查两端的路由表中是否存在对端路由。
- 如果可以 ping 通，则说明隧道两端之间有可达路由。请恢复接口上配置的 IPSec 策略后，执行步骤 8。

步骤 8 检查 IKE peer 配置是否正确。

执行 **display ike peer** 命令，检查项目如下图所示：

版权所有 © 华为技术有限公司

检查项	判断方法及后续操作步骤
Exchange mode	对于 IKEv1 版本，第一阶段的协商模式必须为野蛮模式，否则请执行 **exchange-mode aggressive** 命令修改配置。
Negotiated IKE version	IKE 版本必须相同，如果不相同，请执行 **ike peer** 命令修改配置。
Peer ip address Local ip address	隧道一端的 IKE peer 的 **Peer ip address** 应该等于隧道另一端的 IKE peer 的 **Local ip address**。隧道一端的 IKE peer 的 **Local ip address** 应该等于隧道另一端的 IKE peer 的 **Peer ip address**。如果不匹配，请执行 **local-address** 命令修改 IKE 本端 IP 地址。
remote-name	对端名称必须与对端的本地名称一致，如果不匹配，请执行 **remote-name** 命令来修改配置。
NAT-traversal	必须使能 NAT 穿越功能，如果没有使能，请执行 **nat traversal** 命令使能 NAT 穿越功能。
Local id type	本地 IKE 的 ID 类型必须为 name，如果不是，请执行 **local-id-type** 命令修改配置
Peer id type	对于 IKEv2 版本，远端的 peer IKE 的 ID 类型必须为 name，如果不是，请执行 **peer-id-type** 命令修改配置。

如果 IKE peer 配置正确，请执行步骤 9。

步骤 9 检查 IPSec 隧道两端对等体的 IKE 安全提议是否一致。

分别在两端设备上执行 **display ike proposal** 命令，两端 IKE 安全提议的配置应该保持一致。

- 如果两端的 IKE 安全提议不一致，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》重新配置 IKE 安全提议。
- 如果两端的 IKE 安全提议一致，请执行步骤 2。

说明

如果将认证方式设置为预共享密钥认证方式，则需要为每个对端配置预共享密钥，且建立安全连接的两个对端的预共享密钥必须一致，如果两端不一致，请执行 **pre-shared-key** 命令修改 pre-shared key 认证方法的认证字。

步骤 10 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

版权所有 © 华为技术有限公司

相关日志

无

12.2.5 GRE over IPSec 的定位思路

常见原因

本类故障的常见原因主要包括：

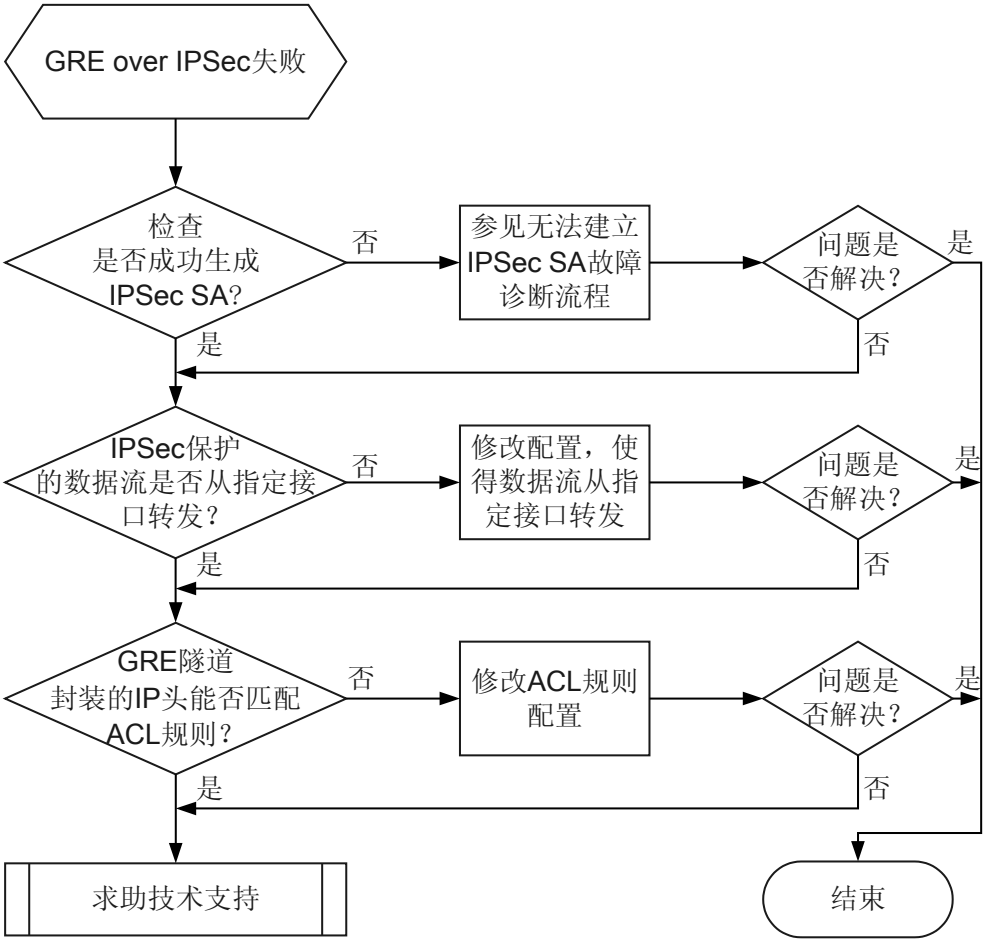
- 链路故障
- 数据流未从指定接口转发
- GRE 隧道封装的 IP 头不匹配 IPSec 策略引用的 ACL 规则
- IPSec 隧道两端的安全提议不一致
- IPSec 隧道两端的安全策略是否匹配：如 IPSec 协商模式不一致、PFS 配置不一致
- 安全策略引用的 ACL 规则不互为镜像
- 两端对等体的 IKE 安全提议不一致
- IKE peer 配置不正确：如 IKE 协商模式不相同、IKE 版本不相同、IKE peer 的 IP 地址不匹配、IKE peer 的对端名称不匹配

故障诊断流程

详细处理流程如图 12-15 所示。

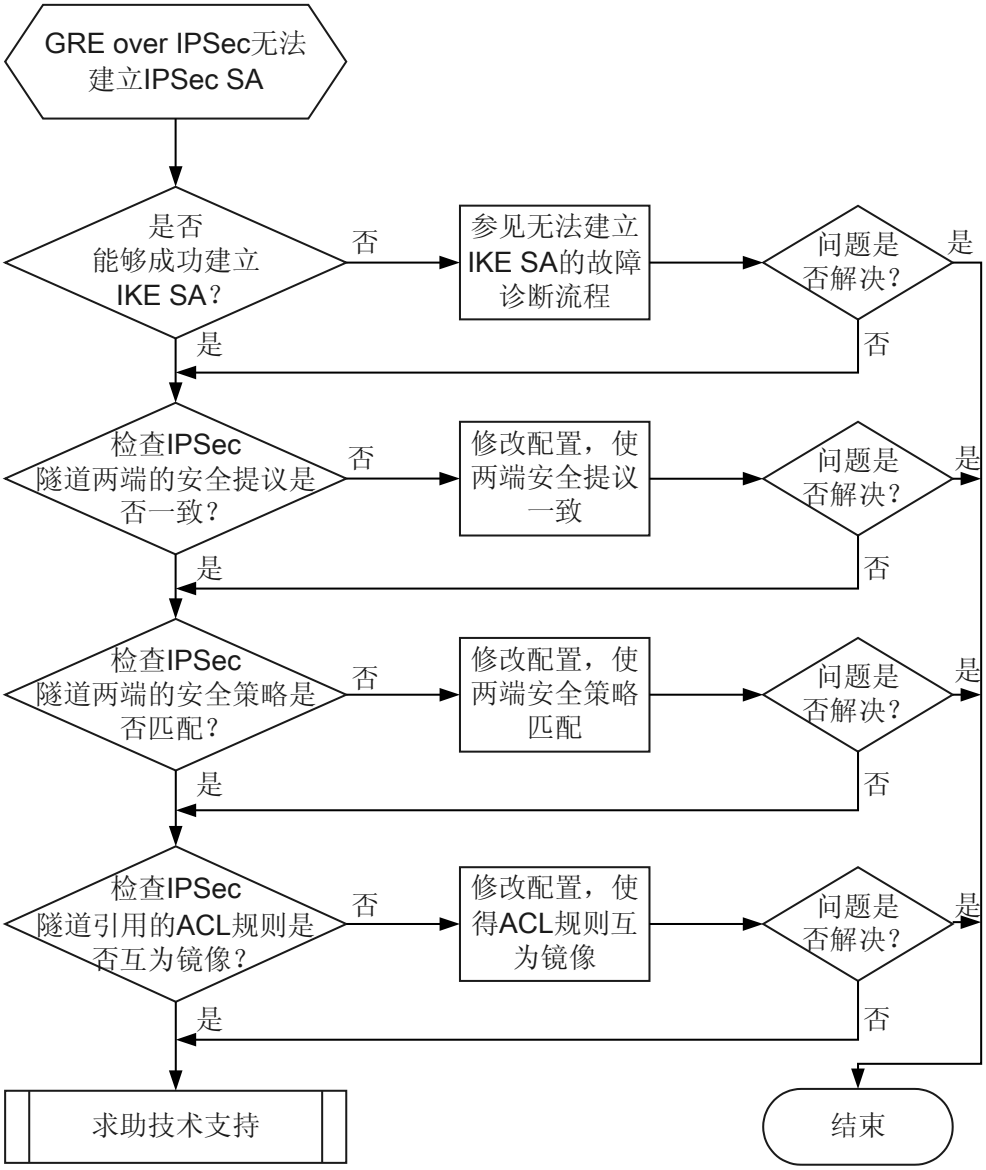
版权所有 © 华为技术有限公司

图 12-15 GRE over IPSec 失败的故障诊断流程图



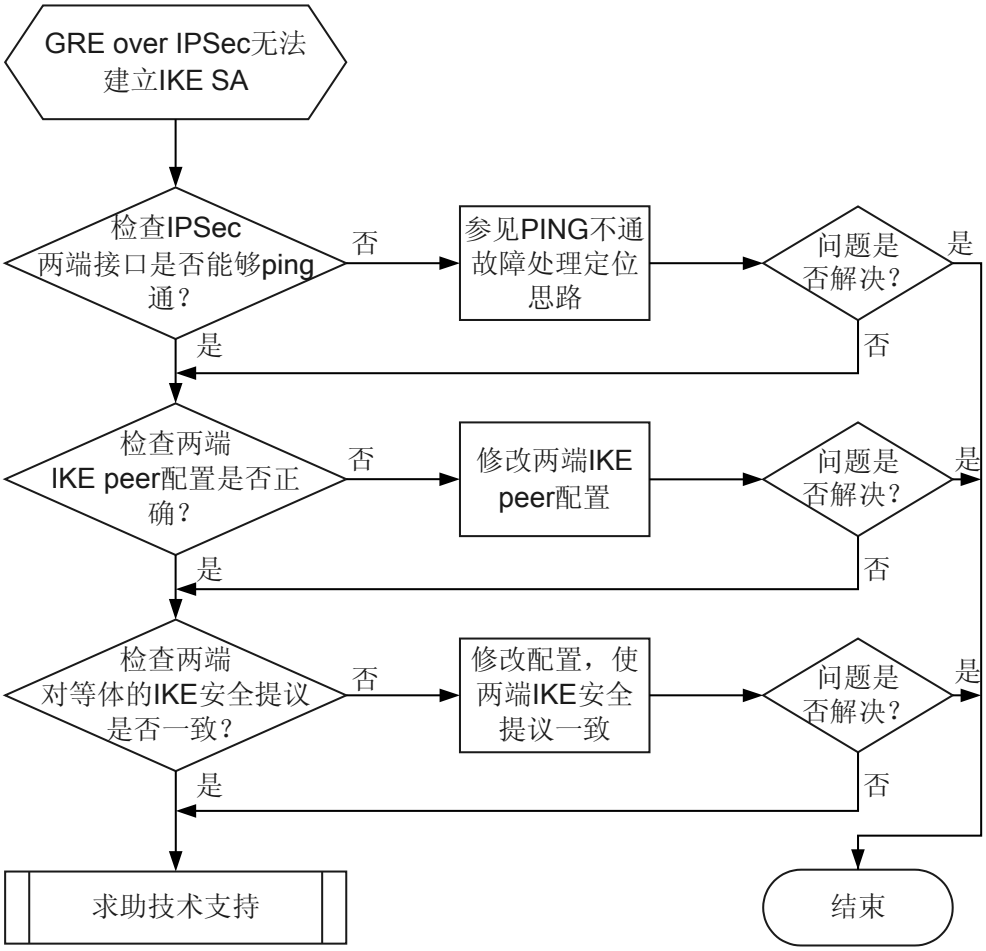
版权所有 © 华为技术有限公司

图 12-16 GRE over IPSec 无法建立 IPSec SA 的故障诊断流程图



版权所有 © 华为技术有限公司

图 12-17 GRE over IPSec 无法建立 IKE SA 的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查是否成功建立生成 IPSec SA 和 IKE SA。

执行 **display ike sa** 命令，通过查看 **Peer**、**Flag** 和 **Phase** 字段可知哪些对等体建立了哪个阶段的 SA。显示信息如下可知，IP 地址为 30.0.0.1 的 Peer 第一阶段协商建立了 IKE SA，第二阶段协商建立了 IPSec SA。

```
<RouterA>display ike sa
    Conn-ID  Peer            VPN   Flag(s)                 Phase
-------------------------------------------------------------------
    397      30.0.0.1        0     RD                      2
    367      30.0.0.1        0     RD                      1

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
```

说明

如果两端配置的 IKE 版本是 v1，使用命令 **display ike sa**。如果两端配置的 IKE 版本是 v2，使用命令 **display ike sa v2**。

版权所有 © 华为技术有限公司

- 如果成功建立了 IPSec SA 和 IKE SA，请执行步骤 2。
- 如果未成功建立 IPSec SA，但是成功建立了 IKE SA，请执行步骤 4。
- 如果未成功建立 IKE SA，请执行步骤 8。

步骤 2 检查 IPSec 隧道保护的数据流是否从指定接口转发。

应确保出方向的数据流通过应用了 IPSec 策略的接口发送。

具体检查方法如下：

- 在两端设备执行 **display ip routing-table** 命令，检查到对端的路由的下一跳可达的出接口是否为指定接口。如果不是指定接口，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IP 路由》修改路由配置。
- 在两端设备执行 **display arp** 命令，检查学习到的对端 IP 地址的 ARP 表项中的接口是否为指定接口。如果不是指定接口，请执行 **reset arp** 命令清除 ARP 映射表中的 ARP 项。

如果数据流是从指定接口转发，请执行步骤 3。

步骤 3 检查数据流是否可以命中流量匹配规则。

通过分析数据流量的源 IP 地址和目的 IP 地址、源端口号和目的端口号等信息，检查 GRE 隧道封装的 IP 头能否匹配 IPSec 策略引用的 ACL 规则。

- 如果数据流不能命中流量匹配规则，报文就进入不了 IPSec 隧道，而被直接转发。请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》进行修改流量匹配规则。
- 如果数据流可以命中，请执行步骤 10。

步骤 4 检查 IPSec 隧道两端的安全提议是否一致。

分别在两端设备上执行 **display ipsec proposal** 命令，查看两端 IPSec 安全提议的配置是否保持一致。具体检查项如下表所示：

检查项	检查标准和后续操作方法
IPsec Proposal Name	检查两端 IPSec 安全策略中绑定的提议的是否一致.，如果不一致，请执行 **ipsec proposal** 命令修改配置。
Encapsulation Mode	检查提议采用的模式是否一致，如果不一致，请执行 **encapsulation-mode** { **transport** | **tunnel** } 命令修改配置。
Transform	检查提议采用的安全协议是否一致，如果不一致，请执行 **transform** { **ah** | **esp** | **ah-esp** }命令修改配置。
AH Protocol	检查 AH 协议采用的认证算法是否一致，如果不一致，请执行 **ah authentication-algorithm** { **md5** | **sha1** }命令修改配置。
ESP Protocol	检查 ESP 协议采用的认证算法和加密算法是否一致，如果不一致，请执行 **esp authentication-algorithm** [**md5** | **sha1**]命令修改认证算法，执行 **esp encryption-algorithm** [**3des** | **des** | **aes-128** | **aes-192** | **aes-256**]命令修改加密算法。

如果两端的 IPSec 安全提议一致，请执行步骤 5。

版权所有 © 华为技术有限公司

步骤 5 检查 IPsec 隧道两端的安全策略是否匹配。

请查看下列检查项：

检查项	判断标准及后续操作步骤
IPSec 协商模式	执行 **display ipsec policy brief** 命令查看 **Mode** 字段，两端的协商模式必须保持一致，如果不一致，请执行 **ipsec policy isakmp** 命令修改配置。
DH (Diffie-Hellman)组	如果本端指定了 PFS，对端在发起协商时必须是 PFS 交换，即本端和对端指定的 Diffie-Hellman 组必须一致，否则协商会失败。执行 **display ipsec policy** 命令查看 **Perfect Forward Secrecy** 字段，如果两端配置不一致，请执行 **pfs** { **dh-group1** | **dh-group2** } 修改配置。

如果两端的安全策略匹配，请执行步骤 6。

步骤 6 检查 IPSec 隧道两端安全策略引用的 ACL 是否互为镜像。

说明

IPSec over GRE 如果采用的是安全策略模板方式，在这种情况下可以选择配置或不配置 ACL 规则，如果配置了 ACL 规则，请保证 ACL 规则的匹配。

建议安全策略模板下不配置 ACL 规则。

在两端 Router 上分别执行 **display acl** 命令，如果两端设备作如下显示，说明两端安全策略引用的 ACL 互相镜像。

RouterA 的 ACL 配置信息。

```
<RouterA>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

RouterB 的 ACL 配置信息。

```
<RouterB>display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

- 如果不互为镜像，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》修改配置。
- 如果配置正确，请执行下面的步骤 2。

步骤 7 检查应用 IPSec 隧道两端接口是否能够 ping 通。

请先在 IPSec 隧道两端的 Router 接口上执行 **undo ipsec policy** 命令，将引用的 IPSec 策略删除。然后以一端接口 IP 地址为源 IP，**ping** 另一端的接口 IP 地址，查看是否可以 ping 通。

- 如果不能 ping 通，请参见 **7.1.1 Ping 不通问题的定位思路**检查两端的路由表中是否存在对端路由。
- 如果可以 ping 通，则说明隧道两端之间有可达路由。请恢复接口上配置的 IPSec 策略后，执行步骤 8。

步骤 8 检查 IKE peer 配置是否正确。

执行 **display ike peer** 命令，检查项目如下图所示：

版权所有 © 华为技术有限公司

检查项	判断方法及后续操作步骤
Exchange mode	第一阶段的协商模式即 IKE 协商模式必须相同，如果不相同，请执行 **exchange-mode** { **main** | **aggressive** }命令修改配置。
Negotiated IKE version	IKE 版本必须相同，如果不相同，请执行 **ike peer** 命令修改配置。
Peer ip address Local ip address	隧道一端的 IKE peer 的 **Peer ip address** 应该等于隧道另一端的 IKE peer 的 **Local ip address**。隧道一端的 IKE peer 的 **Local ip address** 应该等于隧道另一端的 IKE peer 的 **Peer ip address**。如果不匹配，请执行 **local-address** 命令修改 IKE 本端 IP 地址，执行 **remote-address** 命令修改 IKE peer 对端的 IP 地址。
remote-name	对端名称必须与对端的本地名称一致，如果不匹配，请执行 **remote-name** 命令来修改配置。 **说明** 以下情况会使用对端名称: ● IKEv1 版本时，协商模式为野蛮模式下且使用名字认证的情况下 ● IKEv2 版本时，当远端的 peer IKE 的 ID 类型为 name 的情况下

如果 IKE peer 配置正确，请执行步骤 9。

步骤 9 检查 IPSec 隧道两端对等体的 IKE 安全提议是否一致。

分别在两端设备上执行 **display ike proposal** 命令，两端 IKE 安全提议的配置应该保持一致。

- 如果两端的 IKE 安全提议不一致，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》重新配置 IKE 安全提议。
- 如果两端的 IKE 安全提议一致，请执行步骤 2。

说明

如果将认证方式设置为预共享密钥认证方式，则需要为每个对端配置预共享密钥，且建立安全连接的两个对端的预共享密钥必须一致，如果两端不一致，请执行 **pre-shared-key** 命令修改 pre-shared key 认证方法的认证字。

步骤 10 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

12.2.6 采用 IPSec 虚拟隧道方式无法建立安全联盟的定位思路

常见原因

本类故障的常见原因主要包括：

- 链路故障
- IPSec 虚拟隧道配置不正确
- IPSec 隧道两端的安全提议不一致
- IPSec 隧道两端的安全框架是否匹配：如 PFS 配置不一致
- 两端对等体的 IKE 安全提议不一致
- IKE peer 配置不正确：如 IKE 协商模式不相同、IKE 版本不相同、IKE peer 的 IP 地址不匹配、IKE peer 的对端名称不匹配

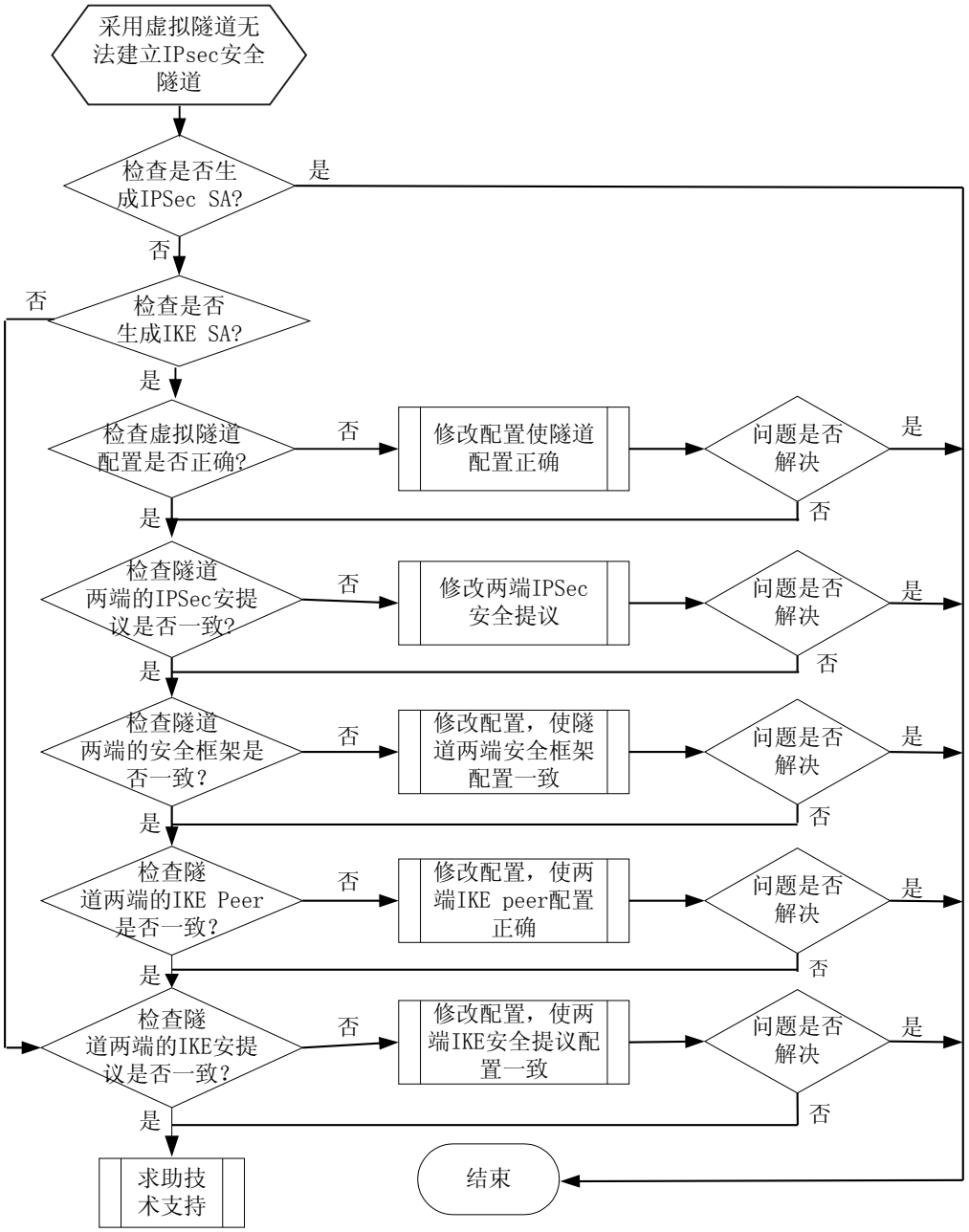
故障诊断流程

在 IPSec 虚拟隧道方式配置 IPSec 后，发现 IPSec 无法对数据进行保护。

详细处理流程如图 12-18 所示。

版权所有 © 华为技术有限公司

图 12-18 采用 IPSec 虚拟隧道方式建立安全联盟的故障诊断流程图



故障处理步骤

说明

请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。

操作步骤

步骤 1 检查是否成功建立生成 IPSec SA 和 IKE SA。

执行 **display ike sa** [**v2**]命令，通过查看 **Peer**、**Flag** 和 **Phase** 字段可知哪些对等体建立了哪个阶段的 SA。显示信息如下可知，IP 地址为 30.0.0.1 的 Peer 第一阶段协商建立了 IKE SA，第二阶段协商建立了 IPSec SA。

版权所有 © 华为技术有限公司

```
<RouterA>display ike sa
    Conn-ID  Peer            VPN    Flag(s)                 Phase
-------------------------------------------------------------------
    397      30.0.0.1        0      RD                      2
    367      30.0.0.1        0      RD                      1

  Flag Description:
  RD--READY    ST--STAYALIVE    RL--REPLACED    FD--FADING    TO--TIMEOUT
  HRT--HEARTBEAT    LKG--LAST KNOWN GOOD SEQ NO.    BCK--BACKED UP
```

- 如果成功建立了 IPSec SA 和 IKE SA，则说明协商成功。
- 如果未成功建立 IPSec SA，但是成功建立了 IKE SA，请执行步骤 2。
- 如果未成功建立 IKE SA，请执行步骤 6。

步骤 2 检查应用 IPSec 隧道两端的 tunnel 接口配置是否正确。

请先在 IPSec 隧道两端的 tunnel 接口上执行 **undo ipsec profile** 命令，将引用的 IPSec 框架删除，检查两端 tunnel 接口配置是否正确。

- – 如果是 GRE Tunnel 口，以一端接口 IP 地址为源 IP，**ping** 另一端的接口 IP 地址，查看是否可以 ping 通。如果不能 ping 通，请检查 GRE Tunnel 口的源地址和目的地址是否配置正确。

  说明

  IPSec Tunnel 口的两端源地址和目的地址都必须配全。

- – 如果是 IPSec Tunnel 口，检查两端 Tunnel 口配置是否正确。IPSec Tunnel 口的两端，其中有一端接口的源地址和目的地址必须配全，则另一端可以不用配置目的地址，并且 Tunnel 口的源地址必须为实际的物理接口地址，也就是 IPSec 隧道的本端地址。

如果配置正确，请执行步骤 3。

步骤 3 检查 IPSec 隧道两端的安全提议是否一致。

分别在两端设备上执行 **display ipsec proposal** 命令，查看两端 IPSec 安全提议的配置是否保持一致，检查项目如下表所示：

检查项	检查标准和后续操作方法
IPsec Proposal Name	检查两端 IPSec 安全策略中绑定的提议的是否一致，如果不一致，请执行 **ipsec proposal** 命令修改配置。
Encapsulation Mode	检查提议采用的模式是否一致，如果不一致，请执行 **encapsulation-mode** { **transport** | **tunnel** } 命令修改配置。
Transform	检查提议采用的安全协议是否一致，如果不一致，请执行 **transform** { **ah** | **esp** | **ah-esp** }命令修改配置。
AH Protocol	检查 AH 协议采用的认证算法是否一致，如果不一致，请执行 **ah authentication-algorithm** { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** } 命令修改配置。
ESP Protocol	检查 ESP 协议采用的认证算法和加密算法是否一致，如果不一致，请执行 **esp authentication-algorithm** [**md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512**]命令修改认证算法，执行 **esp encryption-algorithm** [**3des** | **des** | **aes-128** | **aes-192** | **aes-256**]命令修改加密算法。

版权所有 © 华为技术有限公司

如果两端的 IPSec 安全提议一致，请执行步骤 4。

步骤 4 检查 IPsec 隧道两端的安全框架是否匹配。

分别在两端设备上执行 **display ipsec profile** 命令，查看两端 IPSec 安全框架的配置是否保持一致。

- 如果两端的安全框架不一致，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》重新配置安全框架。
- 如果两端的安全框架匹配，请执行步骤 5。

步骤 5 检查 IKE peer 配置是否正确。

执行 **display ike peer** 命令，检查 IKE 的协商模式、IKE 版本号等信息是否匹配，检查项目如下表所示：

检查项	判断方法及后续操作步骤
Negotiated IKE version	IKE 版本必须相同，如果不相同，请执行 **ike peer** 命令修改配置。
remote-name	对端名称必须与对端的本地名称一致，如果不匹配，请执行 **remote-name** 命令来修改配置。

如果 IKE peer 配置正确，请执行步骤 6。

步骤 6 检查 IPSec 隧道两端对等体的 IKE 安全提议是否一致。

分别在两端设备上执行 **display ike proposal** 命令，两端 IKE 安全提议的配置应该保持一致。

- 如果两端的 IKE 安全提议不一致，请参考《Huawei AR2200-S 系列企业路由器 配置指南-IPSec》重新配置 IKE 安全提议。
- 如果两端的 IKE 安全提议一致，请执行步骤 7。

说明

如果将认证方式设置为预共享密钥认证方式，则需要为每个对端配置预共享密钥，且建立安全连接的两个对端的预共享密钥必须一致，如果两端不一致，请执行 **pre-shared-key** 命令修改 pre-shared key 认证方法的认证字。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司

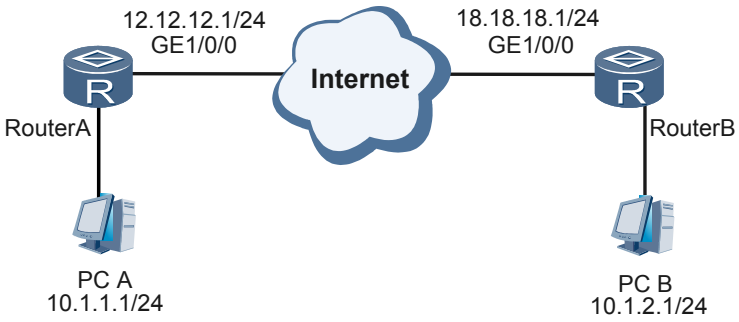
12.2.7 故障处理案例

ACL 配置问题导致手工方式 IPSec 隧道只能单方加解密数据报文

网络环境

如图 12-19，网络中 RouterA 的接口 GE1/0/0 与 RouterB 的接口 GE1/0/0 作为 IPSec 隧道的两个端点，部署 IPSec 业务，保护 PC A 与 PC B 之间的流量。

图 12-19 ACL 配置问题导致手工方式 IPSec 隧道只能单方加解密数据报文的组网图



故障分析

1. 在 RouterA 和 RouterB 上执行 **display ipsec statistics ah/esp** 命令，查看统计计数。发现 RouterA 上只有对入报文做 IPSec 解封装的计数，却没有出报文的统计计数；RouterB 上只有对出报文进行 IPSec 封装的计数，没有对入报文进行 IPSec 解封装的计数。初步判断从 PC A 发向 PC B 的报文在出 RouterA 时没有入 IPSec 隧道。
2. 依次在 RouterA 和 RouterB 上使用命令 **display ipsec sa policy** 查看隧道两端都生成了 inbound 和 outbound 双向的 IPSec SA。且两端 IPSec SA 的协议类型相同，参数 SPI 反向相同，加密和认证密钥也反向相同。确认 SA 没有问题。
3. 使用命令 **display ipsec policy** 查看 RouterA 上的 IPSec 策略下应用的 acl。发现两台 Router 设备都使用了 acl 3101。然后使用 **display acl3101** 检查 ACL 规则。发现两端 ACL 配置的相同。

```
<RouterA> display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 (0 ti
mes matched)
<RouterB> display acl 3101
Advanced ACL  3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 (0 ti
mes matched)
```

操作步骤

步骤 1 在 RouterA 上执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl 3101**，进入 acl 配置。

版权所有 © 华为技术有限公司

步骤 3 执行命令 **undo rule 5**，执行命令 **rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255**。使得 RouterA 和 RouterB 上应用在 IPSec 策略下的 acl 配置反向相同。

步骤 4 执行命令 **return** 退回到用户视图，执行命令 **save**，保存对配置的修改。

步骤 5 完成上述操作后，再使用命令 **display ipsec statistics ah/esp**，查看统计计数，发现故障排除。

----结束

案例总结

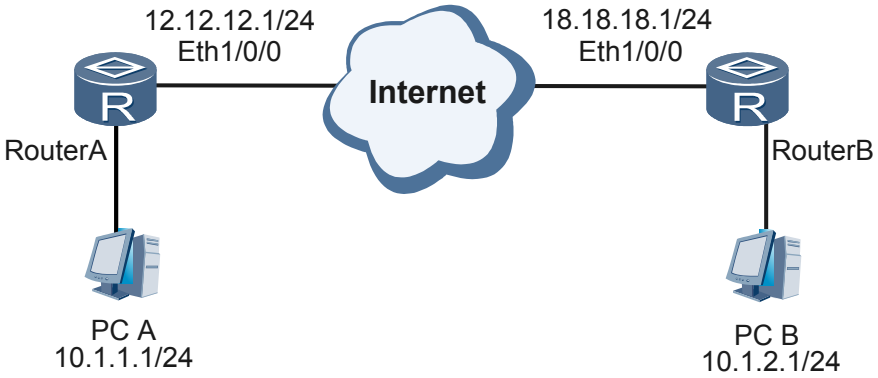
在配置 IPSec 业务时需要注意，需要入 IPSec 隧道的流必须命中 IPSec 策略下应用的 ACL，且隧道两端的 ACL 应该配置成镜像。

安全策略模板方式两端对等体不能协商出安全联盟

网络环境

如图 12-20 所示，在 RouterA 上的接口 GE1/0/0 下应用了 IPSec 策略，在 RouterB 上使用了安全模板方式的 IPSec 策略，保护的是 PC A 与 PC B 之间数据流，IP 报文的封装形式为 tunnel，发现没有协商生成安全联盟。

图 12-20 安全策略模板方式两端对等体不能协商出安全联盟的组网图



故障分析

1. 在 RouterA 和 RouterB 上执行 **display ike sa** 命令，发现没有生成安全联盟。
2. 在 RouterA 上使用命令 **ping** 18.18.18.1，可以 ping 通，说明网络链接正常。
3. 检查两端的 IKE 提议，发现一致。
4. 检查两端的 IPSec 安全提议，发现一致。
5. 检查两端 IPSec 策略的配置。发现 RouterB 接口应用的 IPSec 策略是安全策略模板方式的策略。使用命令 **display ipsec policy** 查看 RouterA 上的 IPSec 策略的配置。RouterA 上的安全策略触发协商方式为流量触发。

```
<RouterA> display ipsec policy name zpolicy005
==========================================
IPsec Policy Group: "zpolicy005"
Using interface: {GE1/0/0}
==========================================
```


版权所有 © 华为技术有限公司

```
    SequenceNumber: 10000
    Security data flow: 3300
    IKE-peer name:  zytpeer
    Perfect forward secrecy: None
    Proposal name:  h
    IPsec SA local duration(time based): 9000 seconds
    IPsec SA local duration(traffic based): 3600 kilobytes
SA trigger mode: Traffic-based
```

由于 RouterB 使用的是模板方式的安全策略，因此不会主动发起协商。RouterA 由于使用了基于流量触发的协商方式，因此它也不会发起协商。所以没有协商生成安全联盟。

操作步骤

- 解决此类故障的方法有两种：
  1. 修改 RouterA 的安全策略的触发方式

     在 RouterA 上进入系统视图后，执行命令 **sa trigger-mode** auto 修改触发方式为自动触发。
  2. 构造数据流触发协商

     在 PC A 上执行命令 **ping** 10.1.2.1，并且命中 IPSec 策略引用的 ACL 规则。

  完成上述操作后，在 RouterA 和 RouterB 上执行 **display ike sa** 命令，发现生成安全联盟，故障排除。

----结束

案例总结

在两端配置 IPSec 策略后，至少需要有一端是主动发起 IKE 协商的，如果本端是安全策略模板方式时，对端必须主动发起协商。发起协商的方式可以是自动协商或按流量触发的协商。

12.3 SSL VPN 故障处理

12.3.1 用户无法登陆 SSL VPN 网关设备的定位思路

常见原因

说明

AR2200-S 作为 SSL VPN 网关设备。

本类故障的常见原因主要包括：

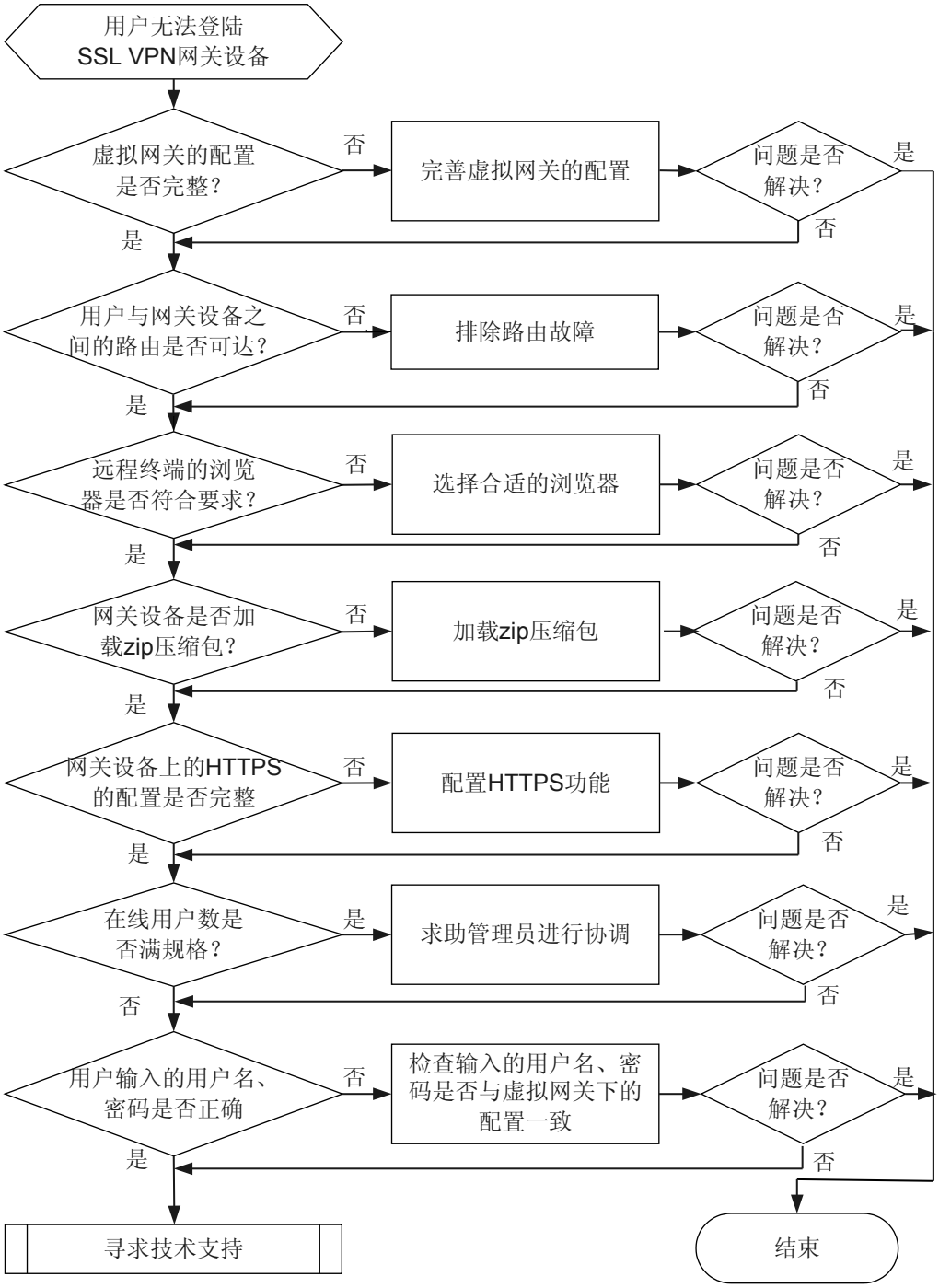
- AR2200-S 上的虚拟网关的配置不完整。
- 用户与 AR2200-S 之间路由有故障，无法互相 ping 通。
- 远程终端的浏览器不是 IE 或 Firefox、浏览器的版本低、浏览器不支持 Javascript 或者浏览器没有启用 cookie 功能。
- AR2200-S 没有加载包含 SSL VPN 网页的 zip 压缩包。
- AR2200-S 上的 HTTPS 的配置不完整。
- 用户输入的用户名、密码不正确。

版权所有 © 华为技术有限公司

故障诊断流程

详细处理流程如图 12-21 所示。

图 12-21 用户无法登陆 SSL VPN 网关设备的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

背景信息

说明

请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。

操作步骤

步骤 1 检查 AR2200-S 虚拟网关的配置是否完整。

- 如果未显示 Web 登录页面，请执行 **display sslvpn gateway** [*gateway-name*]检查虚拟网关是否绑定外网接口、外网接口是否为三层接口且已配置 IP 地址。
- 如果显示 Web 登录页面，但用户没有可选择的虚拟网关，请执行 **display sslvpn gateway** [*gateway-name*]检查虚拟网关是否使能、用户输入的 IP 地址是否与外网接口对应的 IP 地址一致。

如果上述配置未完成，请完成配置。

如果上述配置已完成，请执行步骤 2 检查用户与 AR2200-S 之间的路由是否有故障。

步骤 2 通过 **ping** 检查用户与 AR2200-S 之间的路由是否有故障。

- 如果 ping 不通，请先根据 **7.1.1 Ping 不通问题的定位思路**排除路由的故障。
- 如果能 ping 通，请执行步骤 2。

步骤 3 检查远程终端的浏览器。

远程终端的浏览器必须符合以下要求：

- IE 浏览器（6.0 版本以上）或 Firefox 浏览器（3.0 版本以上）。
- 浏览器支持 Javascript。
- 浏览器启用 cookie 功能。

如果浏览器符合要求，但故障仍存在，请执行步骤 3。

步骤 4 检查 AR2200-S 是否加载了含有 SSL VPN 网页的 zip 压缩包。

在任意视图下执行 **display current-configuration** 命令，查看 AR2200-S 是否存在加载 zip 压缩包的配置。

如下显示信息所示，AR2200-S 上存在加载 zip 压缩包的配置。

```
<Huawei> display current-configuration
 ...
 http server load web.zip
 ...
```

说明

管理员可以任意命名含有 SSL VPN 网页的 zip 压缩包，但该 zip 压缩包中必须包含名称为“sslvpn”的文件夹。

如果 AR2200-S 没有加载含有 SSL VPN 网页的 zip 压缩包，请执行 **http server load** 命令加载。

如果 AR2200-S 加载了含有 SSL VPN 网页的 zip 压缩包，但故障仍存在，请执行步骤 4。

步骤 5 检查 AR2200-S 上的 HTTPS 的配置是否完整。

版权所有 © 华为技术有限公司

说明

执行本步骤前，请确保 AR2200-S 已成功获取数字证书。如果 AR2200-S 没有成功获取数字证书，请根据 **10.8 PKI 故障处理**排除 PKI 故障。

在任意视图下执行 **display current-configuration** 命令，查看 AR2200-S 上的 HTTPS 的配置是否完整。

如下显示信息所示，AR2200-S 上存在 HTTPS 的完整配置。

```
<Huawei> display current-configuration
...
http secure-server ssl-policy user
http secure-server enable
...
```

如果 AR2200-S 不存在 HTTPS 的完整配置，请配置 HTTPS 功能。HTTPS 的详细配置参考《Huawei AR2200-S 系列 企业路由器 配置指南-安全配置》中的 HTTPS 配置。

如果 AR2200-S 存在 HTTPS 的完整配置，但故障仍存在，请执行步骤 5。

步骤 6 检查在线用户数是否满规格。

用户进入 Web 登录页面，点击“登录”按钮，如果浏览器提示在线用户数已满，说明在线用户数已达到整机或者虚拟网关所支持的最大在线用户数。此时，可以通过查看日志进行分析是整机还是虚拟网关达到最大在线用户数，并求助 SSL VPN 网关设备管理员进行协调。

步骤 7 检查输入的用户名、密码是否正确。

用户进入 Web 登录页面，点击“登录”按钮，如果浏览器提示用户名、密码错误，请执行 **display sslvpn gateway** *gateway-name* **access-user** [*user-name*]命令检查输入的用户名、密码是否与虚拟网关所配置的用户信息一致。如果信息一致，请根据 **10.1.1 RADIUS 用户认证失败的定位思路**进一步排除 RADIUS 用户认证失败的故障。

步骤 8 如果故障仍未排除，请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

- SVPN_UM/4/DEVICE_MAX_USER
- SVPN_UM/4/GATEWAY_MAX_USER

12.4 DSVPN 故障处理

版权所有 © 华为技术有限公司

12.4.1 Spoke 向 Hub 注册失败的定位思路

常见原因

本类故障的常见原因主要包括：

- NBMA 地址间没有互通
- Tunnel 接口的状态为 down
- 分支 Spoke 和中心 Hub 的 GRE KEY 值配置不一致
- 中心 Hub 配有认证字符串，分支 Spoke 未配置认证字符串，或者两边配置的认证字符串不一致
- 分支 Spoke 和中心 Hub 的 IPSec profile 配置不一致

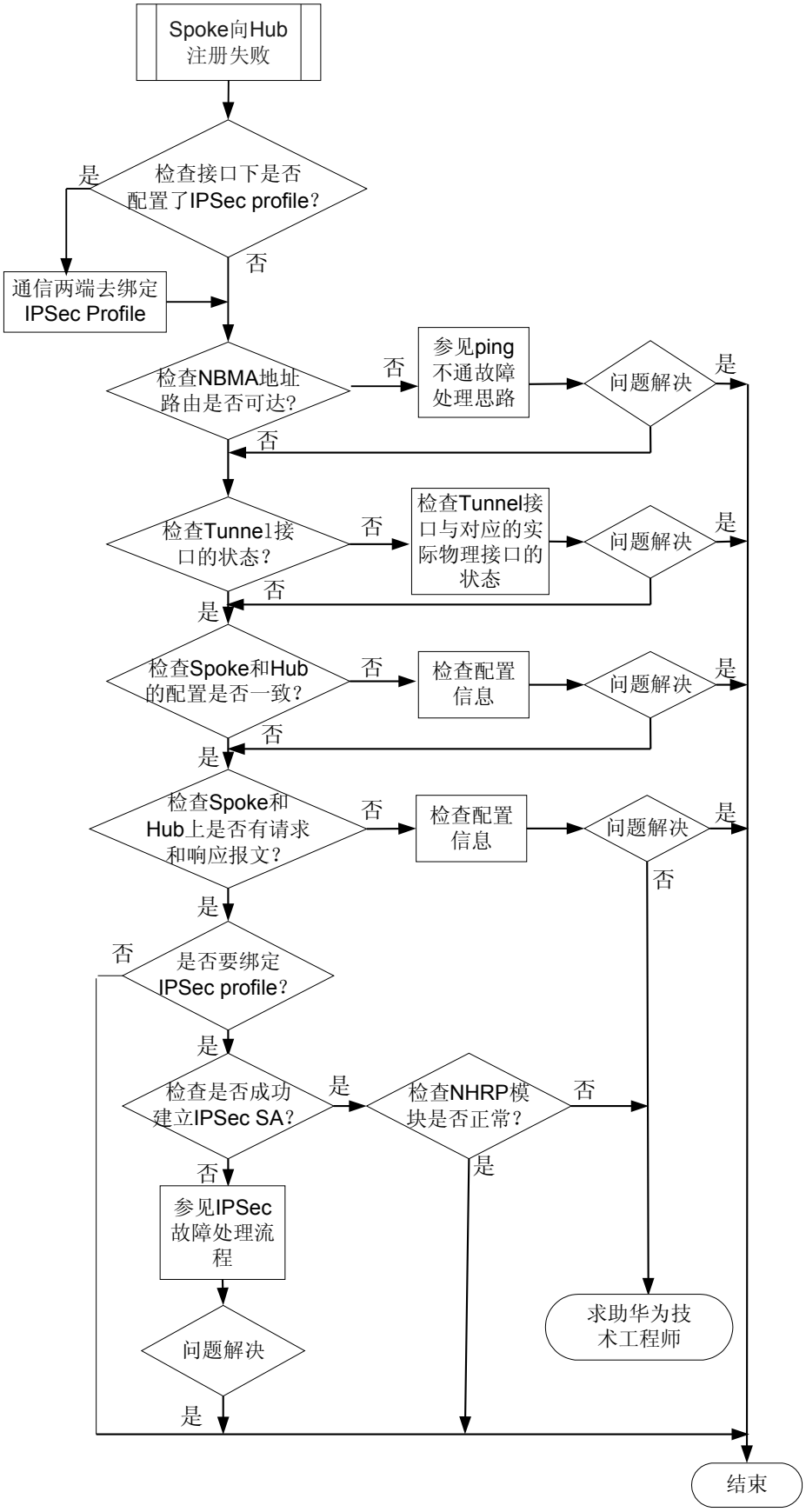
故障诊断流程

在配置 DSVPN 后，发现 Spoke 向 Hub 注册失败。

详细处理流程如图 12-22 所示。

版权所有 © 华为技术有限公司

图 12-22 Spoke 向 Hub 注册失败的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 Spoke-Hub 是否绑定了 IPSec profile。

- 如果 Spoke-Hub 上绑定了 IPSec profile，在接口下执行 **undo ipsec profile** 命令，从接口上取消应用的 IPSec profile，并执行步骤 2。
- 如果 Spoke-Hub 上未绑定 IPSec profile，请执行步骤 2。

步骤 2 检查 Spoke-Spoke,Spoke-Hub 之间是否有可达路由。

在本端 Spoke 上执行 **display ip routing-table** 命令，查看是否含有到对端 Spoke 的路由信息，在 Hub 上执行命令 **display ip routing-table**，查看是否含有到 Spoke 的路由信息。

- 如果 Spoke-Spoke，Spoke-Hub 之间没有可达路由，请检查路由配置。详细的配置方法请参见《Huawei AR2200-S 系列 企业路由器 配置指南-IP 路由》。
- 如果 Spoke-Spoke，Spoke-Hub 之间有可达路由，请执行步骤 3。

步骤 3 检测 Tunnel 接口的状态。

在 Hub 和 Spoke 上，执行 **display interface** *interface-type interface-number* 命令，检查接口当前状态是否 up，如果是 down，执行命令 **undo shutdown** 操作。

如果 Hub 和 Spoke 上的 Tunnel 接口的状态均为 up，请执行步骤 4。

步骤 4 检查 Spoke-Hub 上的配置。

在 Hub 和 Spoke 上，执行 **display nhrp peer** 命令，检查 NHRP Peer 表项。

如果 Hub 上没有对应 Spoke 的动态表项，在 MGRE 接口下执行 **display this** 命令，检查 Hub 和 Spoke 上的配置是否一致。主要检查项目如下表所示：

检查项	检查标准和后续操作方法
nhrp authentication	检查 Spoke 和 Hub 上配置的认证字符串是否一致，如果不一致，请执行 **nhrp authentication** 命令修改配置。
gre key	检查 Spoke 和 Hub 上配置的 GRE 隧道的识别关键字是否一致，如果不一致，请执行 **gre key** 命令修改配置。

如果 Hub 和 Spoke 上的配置均正确，请执行步骤 5。

步骤 5 检查 Spoke 是否发起请求报文，Hub 是否发送回应报文。

在 Spoke 和 Hub 上分别执行 **reset nhrp statistics interface** *interface-type interface-number* 命令，对报文的计数清零。Spoke 重新向 Hub 注册，执行 **display nhrp statistics interface** *interface-type interface-number* 命令，查看请求报文和回应报文数。

- 如果 Spoke 发送注册请求报文失败，RegisterRequestSendSuccess 没有计数，请执行步骤 7。

版权所有 © 华为技术有限公司

- 如果 Spoke 发送注册请求报文成功，RegisterRequestSendSuccess 有计数，但没有收到 Hub 的注册响应报文，RegisterReplyCorrectRecv 没有计数，请执行步骤 7。
- 如果 Spoke 发送注册请求报文成功，且成功收到 Hub 的注册响应报文，中心 Hub 上生成了 Spoke 的 NHRP Peer 表项。此时 Spoke-Hub 上还需要绑定 IPSec profile，请执行步骤 6。

步骤 6 Spoke-Hub 上绑定 IPSec profile。

接口下执行 **ipsec profile** 命令,在接口上应用指定的 IPSec profile，并在 Spoke-Hub 上执行 **display ipsec sa** 命令，查看到隧道两端是否有 IPSec SA 生成。

- 如果隧道两端生成了 IPSec SA，在 Hub 上执行 **display nhrp peer** 命令，查看到 Hub 上未生成 Spoke 的 NHRP Peer 表项，请执行步骤 7。
- 如果隧道两端未生成 IPSec SA，请参见《IPSec 故障处理说明书》。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

12.4.2 分支间进行路由学习场景下 Spoke 与 Spoke 之间无法通信的定位思路

常见原因

本类故障的常见原因主要包括：

- Spoke-Spoke、Hub-Spoke 间子网路由不可达
- Tunnel 接口的状态为 down
- Spoke 在 Hub 上注册失败
- 分支 Spoke 和中心 Hub 的 GRE KEY 值配置不一致
- 中心 Hub 配有认证字符串，分支 Spoke 未配置认证字符串，或者两边配置的认证字符串不一致
- 分支 Spoke 和中心 Hub 的 IPSec profile 配置不一致

故障诊断流程

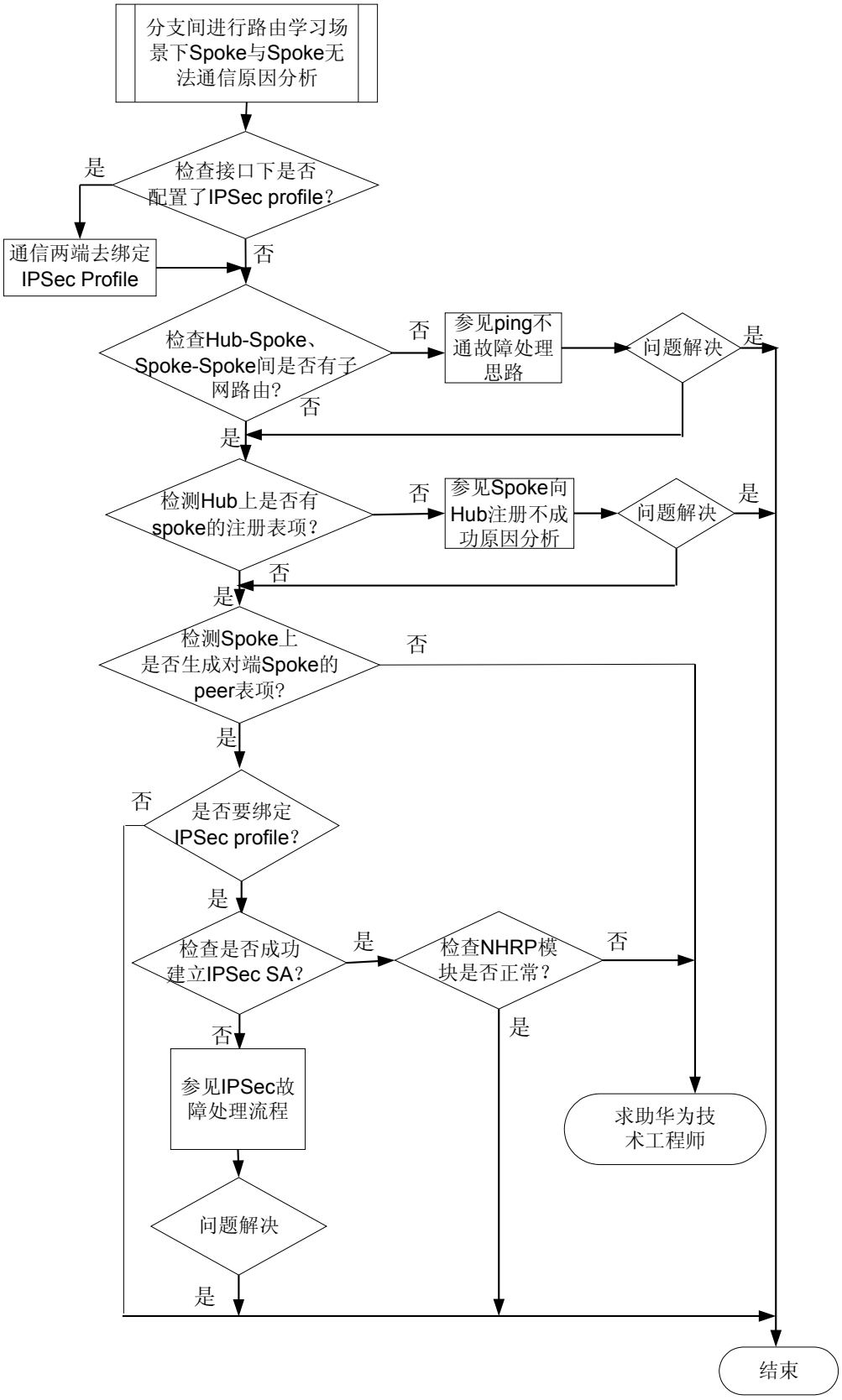
版权所有 © 华为技术有限公司

分支间进行路由学习部署 DSVPN，Spoke 与 Spoke 之间无法通信。

详细处理流程如图 12-23 所示。

版权所有 © 华为技术有限公司

图 12-23 分支间进行路由学习场景下 Spoke 与 Spoke 之间无法通信的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 Spoke-Hub 是否绑定了 IPSec profile。

- 如果 Spoke-Hub 上绑定了 IPSec profile，在接口下执行 **undo ipsec profile** 命令，从接口上取消应用的 IPSec profile，并执行步骤 2。
- 如果 Spoke-Hub 上未绑定 IPSec profile，请执行步骤 2。

步骤 2 检查 Hub-spoke、spoke-spoke 间是否有子网路由。

如果 Spoke 和 Hub 上有子网，在本端 spoke 上执行 **display ip routing-table** 命令，查看是否含有到对端 Spoke 的子网路由信息，在 Hub 上执行 **display ip routing-table** 命令，查看是否含有到 Spoke 子网的路由信息。

- 如果 Hub-spoke、spoke-spoke 间未含有子网的路由信息，请配置到子网的路由信息。详细的配置方法请参见《Huawei AR2200-S 系列 企业路由器 配置指南-IP 路由》。
- 如果 Hub-spoke、spoke-spoke 间含有到子网的路由信息，请执行步骤 3。

步骤 3 检查 Hub 上是否生成了 Spoke 的 peer 表项

在 Hub 上，执行 **display nhrp peer** 命令，查看 nhrp peer 表信息。

- 如果 Hub 上未生成 Spoke 的 peer 表项，请参考 **12.4.1 Spoke 向 Hub 注册失败的定位思路**进行故障排查。
- 如果 Hub 上已经生成了 Spoke 的 peer 表项，请执行步骤 4。

步骤 4 检查两端 Spoke 上是否分别生成了对端 Spoke 的 Peer 表项。

- 在系统视图下执行 **diagnose** 命令，进入诊断视图。
- 执行 **debugging nhrp condition all** 命令，打开调试信息。
- 在 Spoke 上执行 **reset nhrp statistics interface** *interface-type interface-number* 命令，对报文的计数清零，此时从一端 Spoke 向另一端 Spoke 发送流量，执行 **display nhrp statistics interface** *interface-type interface-number* 命令，查看请求报文和回应报文数。
  - 如果 Spoke 发送解析报文失败，ResolutionRequestSendSuccess 没有计数，没有生成 Peer 表项，请执行步骤 6。
  - 如果 Spoke 发送解析报文成功，ResolutionRequestSendSuccess 有计数，且成功收到对端 spoke 的解析回应报文，ResolutionReplyCorrectRecv 有计数，生成了 Peer 表项。此时 Spoke-Hub 上还需要绑定 IPSec profile，请执行步骤 5。

步骤 5 Spoke-Hub 上绑定 IPSec profile。

接口下执行 **ipsec profile** 命令,在接口上应用指定的 IPSec profile，并在 Spoke-Hub 上执行 **display ipsec sa** 命令，查看到隧道两端是否有 IPSec SA 生成。

- 如果隧道两端生成了 IPSec SA，在 Hub 上执行 **display nhrp peer** 命令，查看到 Hub 上未生成 Spoke 的 NHRP Peer 表项，请执行步骤 6。
- 如果隧道两端未生成 IPSec SA，请参见《IPSec 故障处理说明书》。

步骤 6 请收集如下信息，并联系华为技术支持工程师。

版权所有 © 华为技术有限公司

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

12.4.3 分支只有到总部的汇聚路由场景下 Spoke 与 Spoke 之间无法通信的定位思路

常见原因

本类故障的常见原因主要包括：

- Hub-spoke 间子网路由不可达
- Tunnel 接口的状态为 down
- Spoke 在 Hub 上注册失败
- 分支 Spoke 和中心 Hub 的 GRE KEY 值配置不一致
- 中心 Hub 配有认证字符串，分支 Spoke 未配置认证字符串，或者两边配置的认证字符串不一致
- 分支 Spoke 和中心 Hub 的 IPSec profile 配置不一致

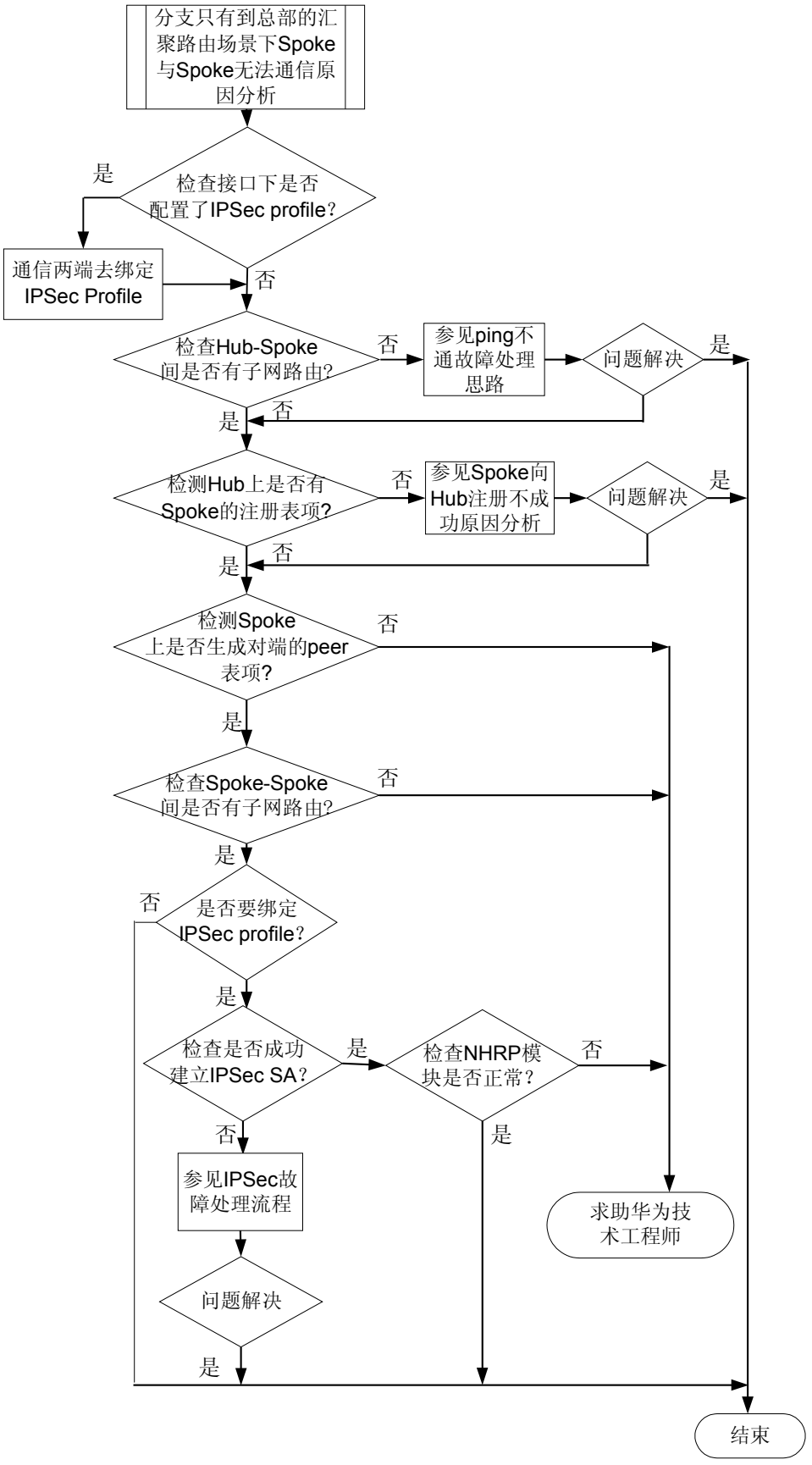
故障诊断流程

分支只有到总部的汇聚路由部署 DSVPN，Spoke 与 Spoke 之间无法通信。

详细处理流程如**图 12-24** 所示。

版权所有 © 华为技术有限公司

图 12-24 分支只有到总部的汇聚路由场景下 Spoke 与 Spoke 之间无法通信的故障诊断流程图



版权所有 © 华为技术有限公司

故障处理步骤

说明

请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。

操作步骤

步骤 1 检查 Spoke-Hub 是否绑定了 IPSec profile。

- 如果 Spoke-Hub 上绑定了 IPSec profile，在接口下执行 **undo ipsec profile** 命令，从接口上取消应用的 IPSec profile，并执行步骤 2。
- 如果 Spoke-Hub 上未绑定 IPSec profile，请执行步骤 2。

步骤 2 检查 Hub-Spoke 间是否有子网路由。

如果 Spoke 和 Hub 上有子网，在 Hub 上执行 **display ip routing-table** 命令，查看是否含有到 Spoke 的子网路由信息。

- 如果 Hub-spoke 间未含有子网的路由信息，请添加到子网的路由信息。详细的配置方法请参见《Huawei AR2200-S 系列 企业路由器 配置指南-IP 路由》。
- 如果 Hub-spoke 间含有到子网的路由信息，请执行步骤 3。

步骤 3 检查 Hub 上是否生成了 Spoke 的 peer 表项

在 Hub 上，执行 **display nhrp peer** 命令，查看 nhrp peer 表信息。

- 如果 Hub 上未生成 Spoke 的 peer 表项，请参考 **12.4.1 Spoke 向 Hub 注册失败的定位思路**进行故障排查。
- 如果 Hub 上已经生成了 Spoke 的 peer 表项，请执行步骤 4。

步骤 4 检查两端 Spoke 上是否分别生成了对端 Spoke 的 Peer 表项。

- 在系统视图下执行 **diagnose** 命令，进入诊断视图。
- 执行 **debugging nhrp condition all** 命令，打开调试信息。
- 在 Spoke 上执行 **reset nhrp statistics interface** *interface-type interface-number* 命令，对报文的计数清零，此时从一端 Spoke 向另一端 Spoke 发送流量，执行 **display nhrp statistics interface** *interface-type interface-number* 命令，查看请求报文和回应报文数。

  本端 Spoke 首次向对端 Spoke 发送流量时，通过调试信息，检测 Hub 上是否触发重定向事件。

  - 如果 Hub 上发送重定向报文失败，RedirectIndicationSendSuccess 没有计数，请执行步骤 7。
  - 如果 Hub 上成功发送重定向报文，RedirectIndicationSendSuccess 有计数，且 spoke 上收到重定向报文，RedirectIndicationCorrectRecv 有计数，但 Spoke-Spoke 间子网路由不可达，请执行步骤 5。

步骤 5 检查 Spoke-Spoke 间是否有子网路由。

当 Spoke 上的 Peer 表项生成后，在本端 Spoke 上执行 **display ip routing-table** 命令，查看是否生成到对端子网的路由信息。

- 如果没有生成到对端子网的路由信息，请执行步骤 7。
- 如果生成了到对端子网的路由信息，Spoke-Hub 上还需要绑定 IPSec profile，请执行步骤 6。

版权所有 © 华为技术有限公司

步骤 6 Spoke-Hub 上绑定 IPSec profile。

接口下执行 **ipsec profile** 命令,在接口上应用指定的 IPSec profile，并在 Spoke-Hub 上执行 **display ipsec sa** 命令，查看到隧道两端是否有 IPSec SA 生成。

- 如果隧道两端生成了 IPSec SA，在 Hub 上执行 **display nhrp peer** 命令，查看到 Hub 上未生成 Spoke 的 NHRP Peer 表项，请执行步骤 7。
- 如果隧道两端未生成 IPSec SA，请参见《IPSec 故障处理说明书》。

步骤 7 请收集如下信息，并联系华为技术支持工程师。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

相关告警与日志

相关告警

无

相关日志

无

版权所有 © 华为技术有限公司